MACHINES ASCENDANT: ROBOTS AND THE RULES OF EVIDENCE

Brian Sites*

CITE AS: 3 GEO. L. TECH. REV. 1 (2018)

INTRODUCTION

Once, courts eschewed "the spector [sic] of trial by machine" and the possibility that "each man's sworn testimony may be put to the electronic test."[1] Judges worried "jurors w[ould] abdicate their responsibility for determining credibility, and rely instead upon the assessment of a machine."[2] Forty years later, that fear has metamorphosed into trusting, even welcoming, machine evidence in place of human accusers.[3] But these "machine accusers," as creations of the imperfect, are fallible. And as tools operated by imperfect human agents, even an otherwise neutral machine can advance an ulterior agenda.[4] Machines

* Associate Professor, Barry University Law School, LL.M. Columbia University Law School, J.D., Florida State University College of Law. I am deeply thankful to: Barry University Law School for supporting this article with a research grant; Michael McGinniss, Michael Morley, and Mark Summers, who offered helpful discussion on this topic previously; my research assistants, Jennifer Barron and Richard Pallas; and the forensic analysts who spoke with me about this article; and the Georgetown Law Technology Review for their helpful edits. Any mistakes herein are my own.

[1] United States v. Bursten, 560 F.2d 779, 785 (7th Cir. 1977); *see also* Andrea Roth, *Trial by Machine*, 104 GEO. L. J. 1245, 1247 (2016) (citing *Bursten*, 560 F.2d at 785).

[2] *Bursten*, 560 F.2d at 785.

[3] *See infra* Part II (discussing cases).

[4] *See, e.g.*, Williams v. Illinois, 567 U.S. 50, 95–96 (2012) (Breyer, J., concurring) (stating that lab procedures have often been abused and listing sources in support of that observation); Pamela R. Metzger, *Cheating the Constitution*, 59 VAND. L. REV. 475 *passim* (2006) (same); *Featured Cases: Exonerated by DNA,* INNOCENCE PROJECT, https://www.innocenceproject.org/all-cases/#exonerated-by-dna [https://perma.cc/99MN-N9LM] (describing analysis of 363 post-conviction exonerations and attributing "unvalidated or improper forensic science" as "play[ing] a role in 49 percent of wrongful convictions later overturned by DNA testing"); Roma Khanna & Steve McVicker, *Probe Finds Crime Lab Faked Results in 4 Cases*, HOUS. CHRON. (June 1, 2005, 5:30 AM), http://www.chron.com/news/houston-texas/article/Probe-finds-crime-lab-faked-results-in-4-cases-1494739.php (noting, *e.g.*, that one of the analysts continued to work at the lab

warrant no blind faith, and whatever trust they receive must be earned through the crucible of the rules of evidence.

Today's robotic offerings look increasingly like the science fiction of years past, and their ascendance has only just begun. Trial by machine is now quite present. In a world where machines increasingly assume the "accuser" roles previously filled primarily by human actors in criminal trials, how do the rules of evidence apply? What rights does a criminal defendant have as to robotic accusers? Who must testify to authenticate machine-generated testimony? What are the consequences of defining statements made by machines as non-hearsay accusatory statements? This article analyzes these questions in the criminal context.

The number of potential machine accusers directly relevant to criminal proceedings is staggering. In an era of "second generation forensic evidence,"[5] circuit-board creep is on the rise as robotics and automation entangle further with society generally and the criminal justice system in particular. A far-from-exhaustive list of machine accusers now includes: machines that map crime scenes via laser imaging and computer software;[6] facial recognition programs used by law enforcement and others;[7] other biometric-based recognition tools such as tattoo recognition;[8] devices that locate cell phones (e.g., Stingrays);[9] automated

---

years later). Machines can also make mistakes on their own. *See, e.g.*, David Kravets, *License Plate Reader Error Leads to Traffic Stop at Gunpoint, Court Case*, ARSTECHNICA (May 12, 2014, 5:43 PM), http://arstechnica.com/tech-policy/2014/05/after-being-held-at-gunpoint-due-to-lpr-error-woman-gets-day-in-court/ [https://perma.cc/5Q43-S7NS].

[5] *See* Erin Murphy, *The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence*, 95 CAL. L. REV. 721, 726–31 (2007) (defining "second generation forensic evidence" such as cell-site location, GPS tracking, biometrics, etc.).

[6] Mauricio Marin, *[North Las Vegas] Police Have New Crime-Solving Tool*, LAS VEGAS NOW (June 23, 2017, 3:00 PM), http://www.lasvegasnow.com/news/nlv-police-have-new-crime-solving-tool/749450915 [https://perma.cc/2CK6-UM8A].

[7] *See, e.g.*, Natasha Singer, *Never Forgetting a Face*, N.Y. TIMES (May 17, 2014), https://www.nytimes.com/2014/05/18/technology/never-forgetting-a-face.html [https://perma.cc/D36D-B2GP] (noting use of facial recognition in law enforcement in New York, Pennsylvania, and California, and also by casinos, grocery stores, and others); Andrew Flanagan, *Thanks To AI, a 3rd Person Is Arrested Following a Pop Superstar's Concert*, NPR (May 23, 2018, 4:15 PM), https://www.npr.org/sections/therecord/2018/05/23/613692526/thanks-to-ai-a-3rd-person-is-arrested-following-a-pop-superstars-concert [https://perma.cc/U2U8-98QZ] (describing facial recognition software's use in China and noting "Amazon has been shopping its own facial recognition technology . . . to U.S. law enforcement").

[8] *See, e.g.*, *Street-Level Surveillance: Tattoo Recognition*, ELEC. FREEDOM FOUND., https://www.eff.org/pages/tattoo-recognition [https://perma.cc/7MUZ-VKDL] (describing the technology as "still in its infancy, [but] . . . being actively developed by

license plate readers;[10] stoplight cameras;[11] drug-, firearm-, and general crime-detecting devices;[12] software that estimates a defendant's "future dangerousness" in the context of sentencing and parole;[13] and innumerable laboratory machines that produce increasingly automated results on topics ranging from DNA to drugs.[14] Sometimes machines do what humans can do as well; in that situation, should a criminal defendant's rights turn on whether the prosecution employs a man instead of a machine? But machines allegedly also do what even skilled humans generally cannot;[15] against such an accuser, the right to test the evidence is essential.

---

private companies with the support of federal agencies, state law enforcement, and universities").

[9] *See, e.g.*, Tom Jackman, *Police Use of 'StingRay' Cellphone Tracker Requires Search Warrant, Appeals Court Rules*, WASH. POST (Sept. 21, 2017), https://www.washingtonpost.com/news/true-crime/wp/2017/09/21/police-use-of-stingray-cellphone-tracker-requires-search-warrant-appeals-court-rules/ [https://perma.cc/7TAL-ED5K] (discussing StingRay usage as widespread).

[10] *See, e.g.*, Josh Shannon, *Newark Police Expanding Network of Automatic License Plate Readers*, NEWARK POST (Mar. 14, 2018), http://www.newarkpostonline.com/news/newark-police-expanding-network-of-automatic-license-plate-readers/article_cb2b9a42-4efc-50ce-ba49-7822c8e89877.html [https://perma.cc/66KR-MQM6].

[11] *See, e.g.*, Charlie Lapastora, *Red-Light Cameras Come Under Fire, at Least 7 States Trying to Ban Them*, FOX NEWS (Jan. 31, 2018), http://www.foxnews.com/us/2018/01/31/red-light-cameras-come-under-fire-at-least-7-states-trying-to-ban-them.html [https://perma.cc/42HK-B9LL] (noting that "[m]ore than 500 communities in the U.S. have some type of red light or speed camera program").

[12] *See, e.g.*, Lexy Savvides, *Crime-Fighting Robot Can Detect Weapons in Crowd*, CNET (Sept. 21, 2017, 10:00 AM), https://www.cnet.com/news/knightscope-security-robot-can-detect-weapons-in-a-crowd; Sharon Weinberger, *Terrorist 'Pre-Crime' Detector Field Tested in United States*, NATURE (May 27, 2011), https://www.nature.com/news/2011/110527/full/news.2011.323.html [https://perma.cc/N8YU-FGBY]; Chris Weller, *There's a Secret Technology in 90 US Cities that Listens for Gunfire 24/7*, BUS. INSIDER (June 27, 2017, 10:59 AM), http://www.businessinsider.com/how-shotspotter-works-microphones-detecting-gunshots-2017-6 [https://perma.cc/Y8H9-2CXS]; *Future Attribute Screening Technology Fact Sheet*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/publication/future-attribute-screening-technology [https://perma.cc/8JVF-B8GL].

[13] *See, e.g.*, CHRISTOPHER SLOBOGIN, PROVING THE UNPROVABLE: THE ROLE OF LAW, SCIENCE, AND SPECULATION IN ADJUDICATING CULPABILITY AND DANGEROUSNESS 101–14 (2007) (discussing future dangerousness). *See generally* Brian Sites, *The Danger of Future Dangerousness in Death Penalty Use*, 34 FLA. ST. U. L. REV. 959, 960 (2007) (discussing future dangerousness analyses).

[14] *See generally* Brian Sites, *Rise of the Machines: Machine-Generated Data and the Confrontation Clause*, 16 COLUM. SCI. & TECH. L. REV. 3736, 51–57 and accompanying footnotes (2014) (describing cases and various forensic tools in the context of the Confrontation Clause).

[15] *See, e.g.*, Joe Palazzolo, *Defense Attorneys Demand Closer Look at Software Used to detect Crime-Scene DNA*, WALL ST. J. (Nov. 18, 2015, 5:17 AM),

Use of these tools is not new, and these questions are no longer theoretical. Almost two decades ago, law enforcement officials scanned tens of thousands of individuals' faces as they attended Super Bowl XXXV, identifying "a handful of petty criminals."[16] Facial recognition software has grown in law enforcement (and private sector) use since the "Snooper Bowl."[17] Now as many as one in every two Americans is in a law enforcement facial recognition network, and one in four state or local police departments can run facial recognition searches.[18] Forensic experts have described probabilistic DNA genotype matching[19] as "becoming regular practice in criminal cases."[20] And everyday machines that we willingly invite into our lives create evidence that can acquit or accuse us of malfeasance.[21] Machine-generated testimony is real and omnipresent in

---

https://www.wsj.com/articles/defense-attorneys-demand-closer-look-at-software-used-to-detect-crime-scene-dna-1447842603 [https://perma.cc/KA45-TSYT] (discussing TrueAllele, "a program that untangles DNA when humans can't" and citing as an example "a recent Commerce Department study of more than 100 crime labs around the country, [which found that] only seven of them were able to correctly untangle a complex DNA mixture"); *see also* Jessica Pishko, *The Impenetrable Program Transforming How Courts Treat DNA Evidence*, WIRED (Nov. 29, 2017, 7:00 AM), https://www.wired.com/story/trueallele-software-transforming-how-courts-treat-dna-evidence/ [https://perma.cc/9VPG-S36C] (describing TrueAllele as a program that can "make connections that elude humans").

[16] *See, e.g.*, Natasha Singer, *Never Forgetting a Face*, N.Y. TIMES (May 17, 2014), https://www.nytimes.com/2014/05/18/technology/never-forgetting-a-face.html [https://perma.cc/D36D-B2GP] (referring to this as "the 'Snooper Bowl' and noting that "no one detailed").

[17] *See, e.g.*, Jennifer Lynch, *Face Off: Law Enforcement Use of Face Recognition Technology*, ELEC. FREEDOM FOUND. (Feb. 18, 2018), https://www.eff.org/wp/law-enforcement-use-face-recognition [https://perma.cc/6AZ3-2JV8] (noting that "law enforcement officers can use mobile devices to capture face recognition-ready photographs of people they stop on the street; surveillance cameras boast real-time face scanning and identification capabilities; and federal, state, and local law enforcement agencies have access to hundreds of millions of images of faces of law-abiding Americans"); Angelica Cabral, *Automatic Facial Recognition Software Helps Police Make an Arrest in the U.K.*, SLATE (June 6, 2017, 4:01 PM), http://www.slate.com/blogs/future_tense/2017/06/06/automatic_facial_recognition_software_helps_police_make_an_arrest_in_the.html [https://perma.cc/8FUH-8MM5].

[18] *See, e.g.*, Clare Garvie, Alvaro Bedoya, & Jonathan Frankle, *The Perpetual Line-up*, GEO. L. CTR. ON PRIVACY & TECH. (Oct. 18, 2016), https://www.perpetuallineup.org/ [https://perma.cc/K37S-6CKJ].

[19] *See, e.g.*, Pishko, *supra* note 15 ("Through probabilistic genotype matching, programs like TrueAllele can sort out the DNA strands presented in [samples that contain the blood of multiple people].").

[20] *Id.* (quoting Jennifer Friedman, a Los Angeles Public Defender's Office forensic expert).

[21] *See, e.g.*, Jacob Gershman, *Prosecutors Say Fitbit Device Exposed Fibbing in Rape Case*, WALL ST. J. (Apr. 21, 2016, 1:53 PM), https://blogs.wsj.com/law/2016/04/21/prosecutors-say-fitbit-device-exposed-fibbing-in-

a sort of perpetual digital line-up, and "in this line-up, it's not a human that points to the suspect—it's an algorithm."[22]

How should the rules of evidence respond to machine accusers? The goal, as in most things, is finding the right balance. Machines are vital tools for investigating crimes. In this digital age, they make crime prevention possible in ways previously inconceivable. They offer the potential of a brighter, safer future, and courts and rulemakers must strike a balance between due scrutiny and an acknowledgment of the realities of how machines are used. Because the courts have thus far concluded that the Confrontation Clause offers little refuge to a criminal defendant faced with machine accusers,[23] the burden falls to the rules of evidence, which have until now proven inadequate when applied to machines. This article analyzes that result.

In Part I, the article briefly reviews the current state of the law under the Confrontation Clause and why the rules of evidence must bear the weight of protecting a criminal defendant's rights; most of that work, however, remains in my prior article.[24] Part II offers a brief primer on robotics under the rules of evidence. Part III describes the approach courts have taken thus far. Finally, Part III also offers proposals as to how to apply the rules of evidence to address the problems raised herein. In doing so, the article focuses on the authentication requirement and statements made by operators and machines together.

As an initial note, there are other avenues through which a criminal defendant might seek protection in court, such as other constitutional rights and rules of disclosure.[25] Similarly, there are other reforms that would improve the fairness of the criminal justice system in a world of evanescent technological evidence; for example, better pre-trial and discovery-phase evidence analysis, especially since many cases never go

---

rape-case/ [https://perma.cc/5LW6-FFH8] (reporting that a Fitbit, worn by a woman who told police she was raped, ultimately provided electronic data that indicated her claim was fabricated, leading to charges against her).

[22] Garvie, *supra* note 18.

[23] *See, e.g.*, Sites, *supra* note 14.

[24] *Id.*

[25] *See* 18 U.S.C. § 3500 (2018). The Jencks Act requires the government to disclose certain prior statements from the witness so as to empower potential impeachment. *See also* Gundersen v. Municipality of Anchorage, 792 P.2d 673, 674–76 (Alaska 1990) ("[W]e hold that due process requires that the defendant be given an opportunity to challenge the reliability of that [breath test] evidence in the simplest and most effective way possible, that is, an independent test [of the defendant's intoxication level]."); *see generally* Brandon L. Garrett, *Constitutional Regulation of Forensic Evidence*, 73 WASH. & LEE L. REV. 1147, 1152 (2016).

to trial.[26] Much ink has now been penned in these areas, and, as such, this article largely reserves comment on those topics.

However, much less has been said about the application of the rules of evidence to machine accusers and hearsay statements made by machine operators through or with machines.[27] Many courts have held that the rules of evidence are the appropriate source of protection for criminal defendants as to these robotic accusers.[28] If so, those rules must play their part appropriately; however, thus far, courts have not held the rules to their text or spirit. Courts often have not required the machine operators to testify even though, in many cases, no one else can establish that the results of the machine came from the proper use of the tool.

Accordingly, the focus here is on the requirements of the rules of evidence, reserving for another day the role of external protections and related doctrines like *Frye*. Although this article focuses on the Federal Rules of Evidence (FRE), in surveying the landscape of cases, state rules of evidence are also addressed as relevant. For the sake of clarity (and brevity), this article reserves for the third installment in this trilogy the question of whether the problems identified are best tackled through revising the rules of evidence, reinterpreting the Confrontation Clause, or some third option.

I. MACHINE-GENERATED DATA & THE CONFRONTATION CLAUSE

The analysis of a criminal defendant's rights as to machine accusers has, thus far, largely focused on the Sixth Amendment's Confrontation Clause. Under a rubric called the "machine-generated testimony doctrine," courts across the nation have held that machine-generated data does not trigger the Confrontation Clause because it is the machines—not the analysts operating them—that make the statements at issue, and machines are not "witnesses" within the meaning of the Confrontation Clause.[29] Courts have reached this conclusion mainly from

---

[26] *See, e.g.*, Erin Murphy, *The Mismatch Between Twenty-First-Century Forensic Evidence and Our Antiquated Criminal Justice System*, 87 S. CAL. L. REV. 633, 639–652 (2014) (discussing these matters).

[27] *Cf.* Andrea Roth, *Machine Testimony*, 126 YALE L.J. 1972, 1976–77 (2017) ("While a handful of scholars have suggested in passing that the reports of a mechanical observer might be assertive claims implicating credibility, legal scholars have not yet explored machine conveyances in depth.") (internal quotation marks omitted).

[28] *See infra* Parts II–III.

[29] *See* Sites, *supra* note 14, at 51–57 (collecting cases); *see also* Peter Nicolas, *But What If the Court Reporter Is Lying? The Right to Confront Hidden Declarants Found in Transcripts of Former Testimony*, 2010 BYU L. REV. 1149, 1192–93 (2010) (noting, while addressing a different issue, that "the Confrontation Clause encompasses only statements by people").

either a general reading of the Clause or from the court's use of the definition of hearsay to limit the reach of the Constitution. As described in my prior article, this broad exclusion of machine accusers from the Confrontation Clause is inconsistent with the Supreme Court's recent treatment of forensic evidence, and it is an exception that could swallow their holdings whole as machines become increasingly widespread and automated.[30] Because the major issues related to machine testimony have largely been analyzed by courts in the context of the Confrontation Clause and are closely tied to it, this section briefly reviews the state of the field in that area.

The machine-generated testimony doctrine's origin story largely begins with *United States v. Washington*.[31] In *Washington*, a police officer pulled over an individual for erratic driving and subsequently obtained a blood sample.[32] The forensic machines that analyzed it produced approximately twenty pages of data,[33] based on which the lab director issued a report stating the blood sample contained intoxicants.[34] The three analysts who actually conducted the tests—the only individuals who knew if the tests were actually run, if the samples were tampered with, if the defendant's sample was the one placed in the machines, etc.—did not testify in court; their supervisor testified based on the data.[35]

At trial, the defendant sought to cross-examine the three analysts themselves, arguing that the lab director's reliance on raw data from tests he neither performed nor observed violated the Confrontation Clause.[36] The trial court disagreed and admitted the testimony.[37] The Fourth Circuit affirmed on appeal,[38] concluding that the defendant had no such right because "the inculpating 'statement'—that [the defendant]'s blood sample contained PCP and alcohol—was made by the machine . . . [and thus was not] subject to the Confrontation Clause."[39]

---

[30] *See generally* Sites, *supra* note 14.
[31] United States v. Washington, 498 F.3d 225 (4th Cir. 2007). Though other cases preceded *Washington*, in the post-*Crawford* world, *Washington* functions as the first test to adopt this analysis. *See, e.g.*, Joe Bourne, *Prosecutorial Use of Forensic Science at Trial: When is a Lab Report Testimonial?*, 93 MINN. L. REV. 1058, 1079–80 (2009) (describing *Washington* as "an analytical angle from which no other court had approached a *Crawford* issue pertaining to forensic science").
[32] *Washington*, 498 F.3d at 227–28.
[33] *Id.*
[34] *Id.*
[35] *Id.* at 228–29.
[36] *Id.*
[37] *Id.* at 227.
[38] *Id.* at 232.
[39] *Id.* at 229–30.

The court also found that there was no value in cross-examining the technicians: the machines made the statements, and the technicians would know only what the machine data said.[40] The Fourth Circuit stressed that if the concern was the reliability of the data, that issue would be properly addressed through the process of authentication of the evidence,[41] and if the defendant wanted to question the technicians on that topic, he should have subpoenaed them.[42] And so the machine-generated testimony doctrine was born.[43]

This doctrine has taken root in a variety of jurisdictions.[44] In *United States v. Blazier*, the Court of Appeals for the Armed Forces went so far as to state that "it is well-settled that under both the Confrontation Clause and the rules of evidence, machine-generated data and printouts are not statements and thus not hearsay—machines are not declarants—and such data is therefore not 'testimonial.'"[45] For example, in *United States v. Moon*, the Seventh Circuit endorsed *Washington*'s approach in a case involving raw data from an infrared spectrometer and a gas chromatograph, two machines often used in forensic labs (among other places).[46] As in *Washington*, *Moon* involved one expert chemist testifying in court based on the data produced by a different analyst.[47] The Seventh Circuit held that the non-testifying chemist's conclusions were testimonial, but the raw data from the machines was not.[48]

Similarly, in *United States v. Lamons*, the Eleventh Circuit held that data produced by a machine memorializing telephone calls was not testimonial because "the witnesses with whom the Confrontation Clause is

---

[40] *Id.* at 230.
[41] *Id.* at 231 (discussing the requirements of laying a foundation).
[42] *Id.* at 231 n.3.
[43] *See, e.g.*, Bourne, *supra* note 31, at 1079–80 (2009).
[44] *See, e.g.*, United States v. Lizarraga-Tirado, 789 F.3d 1107, 1110 (9th Cir. 2015) (citing *Washington* and holding that satellite images and GPS coordinates and markers didn't violate the Confrontation Clause because they were not statements of a person); United States v. Drayton, No. PWG-13-0251, 2014 WL 2919792, at *6 (D. Md. June 26, 2014) ("[A] machine cannot bear witness against an accused within the meaning of the Confrontation Clause . . . . [O]nly a human may be a declarant . . . ."); State v. Salamone, No. 1 CA-CR 16-0204, 2017 WL 2875096, at *4 (Ariz. Ct. App. July 6, 2017) ("Although the chromatograms are certainly evidence against Salamone, as exclusively-machine-generated data they are not out-of-court statements by any person, and thus are not subject to confrontation or hearsay analysis."). *But see* United States v. Ramos-Gonzalez, 664 F.3d 1 (1st Cir. 2011) (concluding, without analyzing the machine-generated testimony doctrine, that the testimony of one analyst about, *inter alia*, the results of a test violated the Confrontation Clause).
[45] United States v. Blazier, 69 M.J. 218, 224 (C.A.A.F. 2010).
[46] United States v. Moon, 512 F.3d 359, 362 (7th Cir. 2008).
[47] *Id.* at 360–61.
[48] *Id.* at 361.

concerned are *human* witnesses," and the data in *Lamons* was the statement of a machine.[49] The Ninth Circuit has agreed as well in the context of satellite images, GPS markers, and coordinates, holding that there was no Confrontation Clause violation because the geographical information was not statements of a person.[50] In *United States v. Crockett*, a federal district court held that "[t]he instrument readouts and printouts" resulting from analysis of cocaine did not implicate the Confrontation Clause or hearsay rule.[51] The doctrine is old enough that it has also arisen in several post-conviction challenges.[52] Given the overall consistency of the above-discussed federal court decisions and the high standard for post-conviction relief, it is not surprising that those post-conviction challenges have largely been rejected.[53]

State courts have generally rejected machine-generated-testimony claims under the Confrontation Clause as well.[54] For example, in *Hamilton v. State*, a Texas court held that the raw data produced by DNA analysis was a machine-generated statement, and "[t]he Confrontation Clause implicates statements made by persons, not machines."[55] In *People v. Lopez*, the Supreme Court of California held that "[b]ecause, unlike a

[49] United States v. Lamons, 532 F.3d 1251, 1260–61, 1263 (11th Cir. 2008) (emphasis in original).
[50] United States v. Lizarraga-Tirado, 789 F.3d 1107, 1110 (9th Cir. 2015).
[51] United States v. Crockett, 586 F. Supp. 2d 877, 885 (E.D. Mich. 2008); *see also* Adams v. United States, No. 09-6152 (GEB), 2011 WL 1792562, at *2–4 (D.N.J. May 10, 2011) (addressing, as an alternative basis for the court's ruling, the merits of a 28 U.S.C. § 2255 habeas corpus claim that alleged error under the Confrontation Clause, and citing *e.g.*, *Washington* and *Moon*).
[52] *See, e.g.*, White v. Davey, No. 2:14-CV-1427-EFB P, 2016 WL 7404761, at *8 (E.D. Cal. Dec. 22, 2016); Fructuoso v. Paramo, No. CV 14-2481 SS, 2016 WL 6839307, at *12–13 (C.D. Cal. Nov. 21, 2016), *judgment entered*, No. CV 14-2481 SS, 2016 WL 6875231 (C.D. Cal. Nov. 21, 2016), *and cert. denied*, No. 17-55073, 2017 WL 3136219 (9th Cir. Apr. 14, 2017); Godoy v. Virginia Dep't of Corr., No. 1:16CV21 (LMB/JFA), 2016 WL 5661938, at *5 (E.D. Va. Sept. 28, 2016), *appeal dismissed sub nom.*, Godoy v. Dir., Virginia Dep't of Corr., 689 F. App'x 164 (4th Cir. 2017).
[53] *See, e.g.*, sources cited *supra* note 52.
[54] *See, e.g.*, Leger v. State, 732 S.E.2d 53, 60 (Ga. 2012) (supervisor may testify about data generated by other analysts); People v. Brown, 918 N.E.2d 927, 931 (N.Y. 2009) ("The . . . report, furthermore, was not 'testimonial' . . . because it consisted of merely machine-generated graphs, charts and numerical data."); State v. Keck, No. 09CA50, 2011 WL 1233196, at *5–6 (Ohio Ct. App. Mar. 30, 2011) (no Confrontation Clause violation where one analyst testified to her analysis, which was based in part on the apparently machine-generated DNA results that another analyst produced); *cf.* State v. Ortiz-Zape, 743 S.E.2d 156, 162 (N.C. 2013) (citing *Washington* and *Moon* approvingly), *cert. denied*, 134 S. Ct. 2660 (2014); State v. Dilboy, 48 A.3d 983, 989 (N.H. 2012) (noting that testimony based on "raw data, such as graphic or numerical computer printouts, . . . [might] not . . . violat[e] . . . the Confrontation Clause").
[55] Hamilton v. State, 300 S.W.3d 14, 21–22 (Tex. Crim. App. 2009).

person, a machine cannot be cross-examined, here the prosecution's introduction into evidence of the machine-generated printouts . . . did not implicate the Sixth Amendment's right to confrontation."[56] The Connecticut Supreme Court reached a similar result.[57]

A clear pattern has emerged for claims involving machine-generated data. Courts considering such claims have reached analogous conclusions for a variety of machines including those producing DNA results,[58] breathalyzer results,[59] urinalysis results,[60] and machine-generated data from equipment outside the lab.[61] Some courts have also reached the same results without specifically discussing machine-generated testimony; these results include decisions based on the general observation that a supervisor may testify about tests performed by other analysts or the specific point that the supervisor may rely on raw data generated by other analysts.[62] Courts, for the most part, appear unconcerned with the rise in number of "witnesses" immune to cross-examination.

---

[56] People v. Lopez, 286 P.3d 469, 478 (Cal. 2012).

[57] State v. Buckland, 96 A.3d 1163, 1172 (Conn. 2014) ("We hold that the machine generated data is not subject to the restrictions imposed by *Crawford*, *Melendez–Diaz*, and *Bullcoming*.").

[58] *See, e.g.*, State v. Gomez, 244 P.3d 1163, 1166–67 (Ariz. 2010); People v. Arauz, 2D Crim. No. B242843, 2013 WL 3357931, at *5 (Cal. Ct. App. July 3, 2013), *cert. denied*, 134 S. Ct. 2664 (2014).

[59] *See* Cranston v. State, 936 N.E.2d 342, 345 (Ind. Ct. App. 2010); People v. Dinardo, 801 N.W.2d 73, 79 (Mich. Ct. App. 2010); Wimbish v. Commonwealth, 658 S.E.2d 715, 719-20 (Va. Ct. App. 2008).

[60] *See* Marshall v. People, 309 P.3d 943, 947 (Colo. 2013); United States v. Bradford, No. 2009-07, 2009 WL 4250093, at *9 (A.F. Ct. Crim. App. Nov. 23, 2009); United States v. Anderson, No. 2009-06, 2009 WL 4250095, at *5 (A.F. Ct. Crim. App. Nov. 23, 2009); United States v. Skrede, No. 2009-09, 2009 WL 4250031, at *3 (A.F. Ct. Crim. App. Nov. 23, 2009).

[61] *See, e.g.*, Stultz v. Artus, No. 04-CV-3170 (RRM), 2013 WL 937830, at *9–10 (E.D.N.Y. 2013) (automated message stating a payphone's phone number was a statement by a machine, which falls outside the scope of the Confrontation Clause); *cf.* Robertson v. Commonwealth, 738 S.E.2d 531, 532–33 (Va. Ct. App. 2013) (en banc) (involving, but not addressing as such, machine-generated prices from a cash register).

[62] *See* Smith v. State, 28 So. 3d 838, 854–55 (Fla. 2009) (per curiam) (discussing this issue and citing *Washington* and *Moon* approvingly); *id.* at 878–80 (Canady, J., concurring) (disagreeing with the Court's opinion on only other issues); Rector v. State, 681 S.E.2d 157, 160 (Ga. 2009) (holding that a toxicologist could testify about tests and results obtained by another doctor because the toxicologist "reviewed the data and testing procedure" and "[a]n expert may base [his] opinions on data gathered by others"); State v. Roach, 95 A.3d 683, 694–99 (N.J. 2014) (an analyst who tested one DNA sample may testify about a DNA match based on results that depended, in part, on testing for a second DNA sample that another analyst generated); Commonwealth v. Yohe, 79 A.3d 520, 540 (Pa. 2013) ("[W]e hold that [the reviewing supervisor] is the analyst who determined Appellant's [blood-alcohol content]. Although he relied on the raw data produced by the lab technicians [who ran the machines] . . . he is the only individual who engaged in the

Washington, decided in 2007, also demonstrated staying power: even after the Supreme Court's intervening landmark cases of *Melendez-Diaz*, *Bullcoming*, and *Williams*, it remains.[63] *Washington*'s petition for certiorari was even still pending when the Court issued *Melendez-Diaz*.[64] Though the Court granted other petitions for certiorari and remanded them for reconsideration, the Court denied the petition in *Washington*.[65] Other courts, considering the issue for the first time or upon reconsideration after the *Williams et al.* decisions, have held that machine-generated data does not trigger a confrontation right.[66]

Against this rise of the machines, a limited resistance has formed—but its future appears tenuous.[67] For example, in one case, *Young v. United States*, the D.C. Circuit found a Confrontation Clause violation where a supervisor gave surrogate testimony about DNA tests that she neither conducted nor was present for; in doing so, the court "emphasize[d] . . . that it is too simplistic to say that the DNA profiles and the [random-match probability] were not hearsay because they were

---

critical comparative analysis of the results of the . . . tests . . . and determined Appellant's BAC."); *see also id.* at 541–42; *cf.* United States v. Hamilton, 413 F.3d 1138, 1142 (10th Cir. 2005) (computer-generated header "was generated instantaneously by the computer without the assistance or input of a person" and so, in the context of the hearsay rules, there was no "statement" or "declarant").

[63] *See, e.g.*, United States v. Summers, 666 F.3d 192, 202–03 (4th Cir. 2011); United States v. Maxwell, 724 F.3d 724, 726–27 (7th Cir. 2013); *see also* United States v. Darden, 656 F. Supp. 2d 560, 563–64 (E.D. Ma. 2009); Hamilton v. State, 300 S.W.3d 14, 21 (Tex. Crim. App. 2009); *Anderson*, 2009 WL 4250095, at *5.

[64] *See* United States v. Washington, 498 F.3d 225 (4th Cir. 2007), *cert. denied*, 557 U.S. 934 (2009).

[65] *See* Washington v. United States, 129 S. Ct. 2856 (2009), *cert. denied*. This does not mean that the Supreme Court necessarily approved of the result in *Washington*, as there are many reasons a court of discretionary jurisdiction might deny review. The point only is that the Court had an opportunity to address the doctrine post-*Melendez-Diaz*, or at least to require the Fourth Circuit to reconsider in light of *Melendez-Diaz*, but declined to do so.

[66] *See, e.g.*, Oliver v. State, No. 14-09-00690-CR, 2010 WL 3307391, at *4 (Tex. App. Aug. 24, 2010); United States v. Drayton, Criminal No. PWG-13-0251, 2014 WL 2919792, at *8–9 (D. Md. June 26, 2014); People v. Lopez, 286 P.3d 469, 478 (Cal. 2012); People v. Revill, No. B233987, 2013 WL 6094307, at *9–13 (Cal. Ct. App. Nov. 20, 2013).

[67] *See, e.g.*, *Washington*, 498 F.3d at 232–35 (Michael, J., dissenting); State v. Roach, 95 A.3d 683, 698–701 (N.J. 2014) (Albin, J., dissenting); *cf.* Pendergrass v. State, 913 N.E.2d 703, 711 (Ind. 2009) (Rucker, J., dissenting) (not addressing the machine-generated testimony doctrine, but stating "despite whatever ambiguity *Melendez–Diaz* may have created on the question of who must testify at trial, it appears to me the opinion is clear enough that a defendant has a constitutional right to confront at the very least the analyst that actually conducts the tests").

'nothing more than the raw data produced by a machine."[68] However, the overwhelming consensus is that machine-generated data does not require the testimony of the analyst who operated the machine; the right to cross-examine machine accusers and their operators under the Confrontation Clause is largely a dead letter. Absent reinterpretation of the Clause, the protections criminal defendants seek in this area fall to the rules of evidence.

II. ROBOTICS & THE RULES OF EVIDENCE: AN FRE PRIMER

The Federal Rules of Evidence (FRE) and their state counterparts offer a variety of protections to a criminal defendant. Though far from exhaustive, this section serves as a primer for some of those protections relevant to machine-generated evidence. In particular, this section discusses rules related to authentication and hearsay.

At an initial level, the authentication/identification requirement helps ensure that evidence is what it is alleged to be.[69] Notably, this protection is not to ensure reliability but relevance. Under FRE Rule 901, "the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is."[70] Thus, the court does not determine that the evidence necessarily is what is claimed: the district court "serves as [a] gatekeeper in assessing whether the proponent has offered a satisfactory foundation from which the jury could reasonably find that the evidence is authentic. The burden to authenticate under Rule 901 is not high—only a prima facie showing is required."[71] The proponent of the evidence need not "rule out all possibilities inconsistent with

[68] Young v. United States, 63 A.3d 1033, 1046 (D.C. Cir. 2013) (quoting United States v. Summers, 666 F.3d 192, 202 (4th Cir. 2011)). The D.C. Circuit went on to state that "the [data at issue] do[es] not stand on [its] own but, instead, ha[s] meaning because [it] amount[s] to a communication by the scientists who produced [it]—the assertion, 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.*; *see also* United States v. Ramos-Gonzalez, 664 F.3d 1, 6 (1st Cir. 2011) (concluding, without analyzing the machine-generated testimony doctrine, that the testimony of one analyst about, *inter alia*, the results of a test violated the Confrontation Clause); *cf.* Martin v. State, 60 A.3d 1100, 1106 (Del. 2013) (lending some support to the right to cross-examine the operating analyst in machine-generated data contexts).

[69] *See generally* FED. R. EVID. 901–03.

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

[71] United States v. Kaixiang Zhu, 854 F.3d 247, 257 (4th Cir. 2017) (quoting United States v. Vidacak, 553 F.3d 344, 349 (4th Cir. 2009)) (internal quotation marks and citations omitted).

authenticity, rather 'the standard for authentication, and hence for admissibility, is one of reasonable likelihood.'"[72]

A common way to authenticate evidence is through calling to the stand a witness familiar with the underlying data or item. For example, the proponent of satellite images generated by Google Earth could meet the authentication burden via "testimony from a Google Earth programmer or a witness who frequently works with and relies on the program."[73] Or, in the case of a lab report, the analyst who ran the tests could testify. As discussed subsequently, however, courts have also accepted the substitute testimony of an analyst or supervisor who did not run, observe, or otherwise participate in the tests.[74]

One way to meet this burden for certain machines is with Rule 901(b)(9), which allows for authentication of "a process or system."[75] This is a two-step process: first, the proponent must provide evidence that describes the process or system, and second, the proponent must establish that the process or system produces accurate results.[76] Examples of machine-generated testimony that fall under the authentication provisions of this subsection include videos, photographs, x-rays, tape recordings, "and other outputs of mechanisms purporting to depict some aspect of reality in" visual or auditory form.[77] It can also apply to mechanisms that transform or analyze data such as statistical studies.[78]

Related to authentication is the establishment of a chain of custody for an item. This is a showing that the item at issue is the same item, in substantially the same condition, as the one seized from the defendant, taken from the crime scene, etc.[79] This showing is often established by testimony from a witness (or multiple witnesses) who have personal knowledge of the item's progression through the chain. Gaps or other issues related to the chain of custody might not preclude the evidence

---

[72] United States v. Espinal-Almeida, 699 F.3d 588, 609 (1st Cir. 2012) (quoting United States v. Savarese, 686 F.3d 1, 11 (1st Cir. 2012)).

[73] United States v. Lizarraga-Tirado, 789 F.3d 1107, 1110 (9th Cir. 2015) (citing CHARLES ALAN WRIGHT & VICTOR JAMES GOLD, FEDERAL PRACTICE & PROCEDURE § 7114 (2000)); *see also* United States v. Espinal-Almeida, 699 F.3d 588, 612–13 (1st Cir. 2012) (testimony concerning GPS usage did not require expert testimony because "someone knowledgeable, trained, and experienced in analyzing GPS devices" testified).

[74] *See* discussion *infra* Sections II.A, II.B; *infra* notes 112–122.

[75] FED. R. EVID. 901(b)(9).

[76] *See, e.g.*, WRIGHT & GOLD, *supra* note 73.

[77] *Id.* (collecting cases).

[78] *Id.* (collecting cases).

[79] *See generally* FED. R. EVID. 901 (Chain of custody is generally "proof that the item in question was in the continuous possession of one person or facility or a secure chain of individuals or facilities during the relevant period, all relatively tamper- and substitution-proof.").

reaching the jury but may instead negatively affect the weight given to the evidence.[80] Courts commonly "presume[] that custodians have preserved the integrity of the evidence absent a sufficient showing of bad faith, ill will, or proof of tampering."[81]

The Federal Rules of Evidence also impose limitations on expert witnesses.[82] Among other requirements, their testimony must be "based on sufficient facts or data," be "the product of reliable principles and methods," and the expert must have "reliably applied the principles and methods to the facts of the case."[83] Many describe the requirements applicable to expert witnesses as formidable: "[t]he new standard exhorts the judge to be an independent gatekeeper. It commands unequivocally . . . that the expert testimony itself and its foundations be scrutinized at each point in the chain from basis to conclusion, for at least some thres[]hold level of reliability."[84]

Hearsay rules also offer criminal defendants potential protections. However, that is generally not the case when facing machine-generated testimony. Hearsay is defined by the FRE in terms of a "person,"[85] thereby excluding machine statements.[86] Thus, in any court that considers machine-generated data to be solely the statement of the machine—as opposed to an assertion by the operator and the machine or through the machine[87]—the hearsay rules offer defendants minimal protection.[88] Further, even where hearsay statements are at issue, the FRE allow experts to rely on inadmissible hearsay statements in forming and testifying to the

---

[80] *See, e.g.*, United States v. Manning, 738 F.3d 937, 944 (8th Cir. 2014).
[81] *Id.* (citing United States v. Brumfield, 686 F.3d 960, 965 (8th Cir. 2012)).
[82] *See generally* FED. R. EVID. 702 (Testimony by Expert Witnesses).
[83] *Id.* at (b)–(d).
[84] FED. R. EVID. 702.
[85] FED. R. EVID. 801(a) ("(a) Statement. 'Statement' means a person's oral assertion, written assertion, or nonverbal conduct, if the person intended it as an assertion."); *id.* 801(b) ("(b) Declarant. 'Declarant' means the person who made the statement."); *see also* United States v. Washington, 498 F.3d 225, 231 (4th Cir. 2007) ("Only a *person* may be a declarant and make a statement. Accordingly, 'nothing 'said' by a machine . . . is hear-say.'"); United States v. Washington, 498 F.3d 225, 230 (4th Cir. 2007) (quoting 4 MUELLER & KIRKPATRICK, FEDERAL EVIDENCE, § 380, at 65 (2d ed.1994)).
[86] *See, e.g.*, Boothe v. Wheeling Police Officer Sherman (Star #155), 190 F. Supp. 3d 788, 793 (N.D. Ill. 2016) (holding that only a person can be a declarant under the hearsay rules and collecting cases).
[87] *See, e.g.*, Sites, *supra* note 14, at 78–93 (discussing this concept in the context of the Confrontation Clause).
[88] *See, e.g.*, United States v. Lizarraga-Tirado, 789 F.3d 1107, 1109–10 (9th Cir. 2015) (satellite image and GPS coordinates and marker were not hearsay because they were automatically generated by a machine, and hearsay rules do not apply to machine statements).

expert's opinion.[89] Thus, even where courts have concluded that statements pertaining to machine-generated testimony are hearsay, they may still be useable by a lab supervisor or other such individual testifying as a surrogate witness at trial.[90]

III. THE ROAD THUS FAR & THE ROAD AHEAD

As noted above, courts have generally classified machine-generated testimony issues not as a constitutional inquiry, but as one for the rules of evidence.[91] While the Confrontation Clause, as currently interpreted, offers little protection against machine-generated data, the options under the rules of evidence are more robust, at least in theory. These options, however, have often proven unable to carry the weight of protecting a defendant's rights. This section illustrates those holdings with a focus on two primary issues: the authentication requirement and application of hearsay rules under the FRE.

A. Hearsay Analysis

A growing number of courts have looked to the hearsay rules in analyzing machine-generated evidence under the FRE. Courts have considered a variety of machine-generated "statements" including Taser reports,[92] satellite images and GPS coordinates,[93] breathalyzer data,[94] forensic lab reports from machines such as gas chromatography/mass spectrometers (GCMS),[95] and more. For example, in *Patterson v. City of Akron*, the Sixth Circuit held that a report generated by a Taser was not hearsay.[96] The court noted that FRE 801(a) defines "statement," in the context of hearsay, as "a *person's* oral assertion, written assertion, or nonverbal conduct, if the person intended it as an assertion."[97] In reaching

[89] FED. R. EVID. 703. Such evidence may even be disclosed to the jury if its probative value substantially outweighs its prejudicial effect. *Id.*
[90] *See, e.g.*, United States v. Blazier, 69 M.J. 218, 225–26 (C.A.A.F. 2010).
[91] *See, e.g.*, *id.*; United States v. Washington, 498 F.3d 225, 231 (4th Cir. 2007).
[92] Patterson v. City of Akron, 619 F. App'x 462, 479–80 (6th Cir. 2015).
[93] United States v. Lizarraga-Tirado, 789 F.3d 1107, 1109 (9th Cir. 2015).
[94] United States v. Ahlstrom, 530 F. App'x 232, 239 (4th Cir. 2013); United States v. Hall, 497 F. App'x 299, 300 (4th Cir. 2012); United States v. Hamblen-Baird, 266 F.R.D. 38, 39–40 (D. Mass. 2010).
[95] Dunn v. State, 665 S.E.2d 377, 381 (Ga. App. Ct. 2008).
[96] *Patterson*, 619 F. App'x at 479–80.
[97] *Id.* at 480 (quoting Fed. R. Evid. 801(a)).

that conclusion, the court drew on six other circuit decisions on the same topic.[98]

Other courts have reached the same result.[99] In *United States v. Lizarraga-Tirado*, the defendant was arrested for illegally crossing the Mexico-United States border, and the case turned in part on whether he was arrested in the United States or Mexico.[100] The defendant argued that he was on the Mexico side of the border; government agents testified that he was in the United States.[101] In support of their assertion that the arrest was on the United States side, the agents testified that they were familiar with the area and that one of them had "contemporaneously recorded the coordinates of defendant's arrest using a handheld GPS device."[102] The government introduced a Google Earth satellite image that depicted the Mexico-United States border and included a marker called a "tack" that the agent asserted reflected the GPS coordinates she recorded during the arrest.[103] Thus, the defendant had an opportunity to cross-examine the machine operator (the agent who operated the GPS and marked the coordinates), ameliorating both hearsay and authentication issues. The defendant argued, however, that more was needed because there was no testimony as to the origin of the satellite images or the "tack" reflecting the GPS coordinates on the handheld device, both of which were allegedly hearsay statements.[104] The court rejected both arguments, holding that the satellite image—like other photographs from less-powerful cameras—"makes no assertion, [and thus] it isn't hearsay."[105]

The tack and GPS coordinate evidence, however, "present[ed] a more difficult question" because they made an assertion as to what was located there.[106] The machine-generated testimony doctrine resolved this as well: the court determined that the tack and coordinates were generated by Google Earth, and thus, they could not be hearsay because they were

---

[98] *Id.* (citing United States v. Lizarraga–Tirado, 789 F.3d 1107, 1109–10 (9th Cir. 2015); United States v. Lamons, 532 F.3d 1251, 1263 (11th Cir. 2008); United States v. Moon, 512 F.3d 359, 362 (7th Cir. 2008); United States v. Washington, 498 F.3d 225, 230 (4th Cir. 2007); United States v. Hamilton, 413 F.3d 1138, 1142 (10th Cir. 2005); United States v. Khorozian, 333 F.3d 498, 506 (3d Cir. 2003)).
[99] *See, e.g.*, United States v. Crockett, 586 F. Supp. 2d 877, 885 (E.D. Mich. 2008).
[100] *Lizarraga-Tirado*, 789 F.3d at 1108.
[101] *Id.*
[102] *Id.*
[103] *Id.*
[104] *Id.*
[105] *Id.* (citing United States v. May, 622 F.2d 1000, 1007 (9th Cir. 1980); United States v. Oaxaca, 569 F.2d 518, 525 (9th Cir. 1978)).
[106] *Lizarraga-Tirado*, 789 F.3d at 1109.

not statements by a person.[107] The court noted that machine-generated statements could raise other "evidentiary concerns," but it concluded that they "are addressed by the rules of authentication."[108] The defendant in *Lizarraga-Tirado* had not raised any such objection, and therefore the court did not fully explore the issue.

These hearsay issues are not as simple as courts have portrayed them to be. Even taking as a given that the FRE appropriately defines hearsay solely as statements by "person[s]," a statement generated by a machine at the operator's command can be seen as the statement of not just the machine but of the machine and the operator together. When applied to machines used to make assertions about the world, this determination should turn on the question of control: how autonomous is the machine's statement?[109] Exercising control over the machine's analysis, such as by determining what test parameters to use, renders the statement a joint statement.[110] In such a scenario, the operator of the machine should be subject to the Confrontation Clause's requirements and hearsay analysis as well. As a result, the machine operator should normally need to testify for the evidence to be admissible. Notably, when that occurs, authentication claims will largely also be satisfied because the operator can help provide "evidence sufficient to support a finding that the item is what the proponent claims it is."[111]

Evidentiary requirements aside, there are practical reasons a defendant (and the court) should favor calling the machine operator. As one commentator noted, operators can commit a host of errors that are routinely important in a criminal justice context:

> [I]magine a person in a room overheard saying "Brrr—it's cold." A party now offers the statement as proof that the room was generally cold. In truth, the room was warm, but the declarant was standing directly in front of an air conditioning duct, a fact that would likely remain hidden absent the declarant's live testimony. In the same respect, a thermometer placed in front of the air duct, if the reading is presented in court as an accurate report of room's temperature, might cause the factfinder to draw the wrong inference.
>
> . . . .

[107] *Id.* at 1109–10 (citing *Washington*, 498 F.3d at 230 and several other cases discussed herein).
[108] *Id.* at 1110.
[109] *See* Sites, *supra* note 14, at 78–93.
[110] *Id.*
[111] FED. R. EVID. 901(a).

> For example, an operator of a breath-alcohol machine who fails to wait long enough after a suspect vomits before commencing the test runs the risk that the machine will mistake residual mouth alcohol for alcohol in deep lung air and inaccurately estimate the suspect's blood-alcohol level. A computer-run DNA analysis on a crime-scene sample contaminated with residue from a suspect's sample may, without correct control tests, falsely convey that the two samples match. "False" inputs might even include the failure to remove inputs that were correct when initially inputted, but have since become outdated. For example, the failure to scrutinize law enforcement databases for old, resolved warrants has led computer systems to falsely report to officers in the field that a suspect has an outstanding warrant. [112]

Calling the operator-analyst to testify gives the defendant a fair opportunity to explore these and many other critical issues. Just as the thermometer "operator" might have erred or misled the machine, so too might other operators. Without testimony from the machine operator, there will often be no way to determine whether the machine produced accurate and relevant results or was misled by factors within the operator's control. That is a risk the criminal justice system should not accept and which would best be solved by requiring machine operators to testify more frequently. Hearsay requirements could help produce that result if machine-generated statements that are the product of the operator and the machine together are not automatically excluded from hearsay requirements.

B. Authentication

Authentication is also a central concern in machine-generated testimony cases. It raises at least two potential obstacles to the admission of evidence: (1) whether the machine "produced scientifically sound results," and (2) whether the sample tested was actually the sample at issue (e.g., the defendant's sample, the sample from the crime scene, etc.).[113] The first issue can be complex if the machine or test used is not

[112] Roth, *supra* note 27, at 1993, 1999 (citing Ernest Sosa, *Knowledge: Instrumental and Testimonial*, *in* THE EPISTEMOLOGY OF TESTIMONY 116, 117 (Jennifer Lackey & Ernest Sosa eds., 2006)).
[113] United States v. Crockett, 586 F. Supp. 2d 877, 886 (E.D. Mich. 2008).

well established,[114] and the second issue might be important in criminal cases involving testing that renders accusatory results.

Consider the case that largely began the doctrine in the realm of the Confrontation Clause: *United States v. Washington*.[115] Although *Washington* was not the first time courts analyzed machine-generated data under the Federal Rules of Evidence, it represents an important landmark. In the same breath that the Fourth Circuit foreclosed Confrontation Clause rights for innumerable present and future defendants, it highlighted the scope of the protections potentially offered by the rules of evidence.

In particular, the Fourth Circuit in *Washington* concluded that the defendant could have advanced an authentication claim under FRE 901.[116] Since the defendant did not raise it below or on appeal, the court held that the lab samples could be introduced via a supervisor who never tested the materials.[117] Similarly, various other courts addressing machine-generated testimony have expressed little-to-no concern over authentication issues, even where no one with first-hand knowledge testified in court that the test results derived from the actual sample at issue.[118]

As noted previously, under FRE Rule 901, "the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is."[119] The court is to "serve[] as [a] gatekeeper in assessing whether the proponent has offered a satisfactory foundation from which the jury could reasonably find that the evidence is authentic."[120] "[T]he standard for authentication, and hence for admissibility, is one of reasonable likelihood."[121] In the face of an authentication challenge and a surrogate analyst, should the court assume that there is a reasonable likelihood that the lab results came from the defendant's sample simply because someone who works in the lab believes that it did? Is the court to presume that, since lab reports normally aren't falsified or erroneous, the lab report "is what the proponent claims"—the results of proper analysis of the defendant's sample?

---

[114] *See id.*

[115] 498 F.3d 225 (4th Cir. 2007) (addressing machine-generated testimony in the context of forensic analysis).

[116] *Id.* at 231.

[117] *Id.*

[118] *See Crockett*, 586 F. Supp. 2d at 886 (raising this issue and noting that it "was not discussed in the cases dealing with admission of laboratory test results through an expert who did not do the testing").

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

[120] United States v. Kaixiang Zhu, 854 F.3d 247, 257 (4th Cir. 2017) (quoting United States v. Vidacak, 553 F.3d 344, 349 (4th Cir. 2009)) (internal quotation marks and citations omitted).

[121] United States v. Savarese, 686 F.3d 1, 11 (1st Cir. 2012).

As one treatise notes, the authentication burden, though minimal, "may require a showing that . . . the input data was accurately placed into the computer by a competent operator or reliable input device. . . . Failure to establish such a foundation justifies exclusion of the computer evidence."[122] Thus, in cases where no witness testified that the sample analyzed was in fact the defendant's sample or that the machine was operated correctly, it is unclear how even the minimal threshold showing is met. How can the proponent have "produce[d] evidence sufficient to support a finding that the item is what the proponent claims it is"[123] if the only people who know if the sample tested was the defendant's did not testify? How can the court know if the machine was operated correctly on an unadulterated sample if the operator did not testify? Similarly, how is a chain of custody demonstrated without testimony from the witness who actually analyzed the sample—how else could the court know that the sample collected was the sample analyzed? Or as one court succinctly stated: "In order for the expert's opinion on . . . the laboratory instrument [results] . . . to be relevant [and satisfy Rules 104 and 901], there must be information in the record to prove what was tested."[124]

There is no reason to apply the more liberal authentication requirements applicable to the introduction of photographs, videos, and the like. While courts generally do not require testimony from the person who took the photograph or filmed the video, testimony is available from someone who can attest, from personal knowledge, that the depiction is a fair and accurate representation.[125] A supervisor or surrogate analyst can offer no such assertion about a lab report generated from a sample they did not test because they lack adequate personal knowledge of whether the test was run as alleged, how it was run, and whether the sample is actually from the source asserted. In summary, if the FRE authentication rules are to have a meaningful role in cases involving machine-generated testimony, the machine operator will need to testify in more cases.

---

[122] 31 CHARLES ALAN WRIGHT ET AL., FEDERAL PRACTICE & PROCEDURE: EVIDENCE § 7114 (1st ed. 2018).

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

[124] United States v. Crockett, 586 F. Supp. 2d 877, 888 (E.D. Mich. 2008) (citing United States v. Grant, 967 F.2d 81, 82–83 (2d Cir. 1992) ("In order for the chemist's testimony to be relevant, there must be some likelihood that the substance tested by the chemist was the substance seized at the airport. The government's failure to establish a chain of custody from the moment the substance was seized to the time it was subjected to laboratory analysis makes this less likely, and thus casts some doubt on the admissibility of the chemist's testimony.")).

[125] *See, e.g.*, United States v. Cejas, 761 F.3d 717, 724 (7th. Cir. 2014).

C. The Road Ahead

These revisions in hearsay and authentication analysis have deep practical roots given the seemingly endless stream of forensic lab scandals.[126] Absent the ability to challenge evidence through channels such as hearsay or authentication, criminal defendants have little ability to protect themselves from analyst malfeasance. For example, although the defendant in *Washington* did not raise an authentication claim, he did raise a hearsay objection.[127] However, the court held that the statement of the machine was not hearsay under the FRE.[128] Thus, even when presented with an opportunity to protect the defendant's right to inquire into the evidence against him, the court failed to recognize the human role in that accusation.

As discussed above, viewing a machine accusation as solely the product of a machine ignores the reality of how many machines operate. For example, the *Washington* court determined that "[w]hether the machines properly reported [drugs in the defendant's system was] . . . dependent solely on the machine" and the "raw data that the machines generated."[129] However, the machine would be the sole arbiter of whether a defendant's sample had drugs in it only if: (1) the analyst operating the machine used the machine correctly,[130] (2) the analyst did not intentionally tamper with the sample,[131] (3) the analyst did not accidentally alter the

---

[126] *See, e.g.*, Chuck Lindell, *Court: Examine if Austin Crime Lab Botched Death Penalty Evidence*, STATESMAN (Oct. 18, 2017), https://www.statesman.com/news/court-examine-austin-crime-lab-botched-death-penalty-evidence/Fue0LIlp74CTWSUXoSrXuO [https://perma.cc/9JS5-CMWP] (noting that, after a Texas Forensic Science Commission audit revealed that some crime lab staff members were improperly trained and "incorrect methods were used to examine DNA samples," the Texas Court of Appeals ordered a lower court to examine a death penalty defendant's allegations of compromised forensic analysis in his case).

[127] United States v. Washington, 498 F.3d 225, 229–32 (4th Cir. 2007).

[128] *Id.*

[129] *Id.* at 230.

[130] *See, e.g.*, Lindell, *supra* note 126.

[131] *See, e.g.*, Rebecca Everett, *Future Cloudy for Thousands of Drug Cases Tested By Sonja Farak, Records Show Tampering Went On For Nearly Nine Years*, DAILY HAMPSHIRE GAZETTE (Jul. 9, 2015), http://www.gazettenet.com/Archives/2015/07/druglabfolo-hg-070815 [https://perma.cc/2Q2B-P96S]; Seth Augenstein, *Oregon State Crime Lab Analyst Under Investigation for Evidence Tampering*, FORENSIC MAG. (Sept. 17, 2015), https://www.forensicmag.com/article/2015/09/oregon-state-crime-lab-analyst-under-investigation-evidence-tampering [https://perma.cc/K6PZ-P2DC]; Khanna & McVicker, *supra* note 4.

sample or err in some other way,[132] and (4) the analyst actually ran any test whatsoever instead of falsifying the results.[133] As the footnotes included for each of those items highlight, there have been innumerable examples demonstrating that no such assumptions are warranted. How could there be when, in the words of one news outlet nearly five years ago, "[o]ver the years, major failures have occurred in more than 100 U.S. labs."[134] And even when "errors" are not at issue, there are additional ways that the lab analysts might undermine the defendant's case (such as withholding exculpatory information).[135]

These issues are not unique to lab analysts and forensic tools. "So long as . . . motives to lie or cheat exist, programmers face the temptation to [do the same]."[136] Whether it is human error or a machine built to lie,[137]

---

[132] *See, e.g.*, Tracey Kaplan, *Crime Lab Uses Wrong Chemical in 2,500 Methamphetamine Tests in Santa Clara County*, MERCURY NEWS (May 5, 2014), https://www.mercurynews.com/2014/05/05/crime-lab-uses-wrong-chemical-in-2500-methamphetamine-tests-in-santa-clara-county/ [https://perma.cc/6JXA-LH6S]; Allison Manning, *Columbus Crime-Lab Error Might Affect 38 Cases*, COLUMBUS DISPATCH (Aug. 8, 2014), https://www.dispatch.com/content/stories/local/2014/08/08/lab-error-might-affect-38-cases.html [https://perma.cc/C86Y-2KSH].

[133] *See, e.g.*, Katie Mettler, *How a Lab Chemist Went From "Superwoman" To Disgraced Saboteur of More Than 20,000 Drug Cases*, WASH. POST (Apr. 21, 2017), https://www.washingtonpost.com/news/morning-mix/wp/2017/04/21/how-a-lab-chemist-went-from-superwoman-to-disgraced-saboteur-of-more-than-20000-drug-cases/ [https://perma.cc/6U22-2GUX] (describing a Massachusetts forensic analyst who falsified results by "not actually testing all the drugs that came before her, forging her co-workers' initials[,] and mixing drug samples so that her shoddy analysis matched the results she gave prosecutors," leading to the dismissal of 21,587 drug cases "tainted by [her] misconduct"); Justin Zaremba, *Lab Tech Allegedly Faked Result in Drug Case; 7,827 Criminal Cases Now In Question*, NJ.COM (Apr. 26, 2016), http://www.nj.com/passaic-county/index.ssf/2016/03/state_police_lab_tech_allegedly_faked_results_in_p.html [https://perma.cc/C5SR-J8UL].

[134] Jordan Michael Smith, *Forget CSI: A Disaster is Happening in America's Crime Labs*, BUS. INSIDER (Apr. 30, 2014), http://www.businessinsider.com/forensic-csi-crime-labs-disaster-2014-4 [https://perma.cc/X4Y5-K7JJ]; *see also Crime Lab and Forensic Scandals*, KOMORN LAW, http://komornlaw.com/crime-lab-and-forensic-scandals/ [https://perma.cc/KH87-SNPW] (listing numerous alleged forensic lab scandals).

[135] *See, e.g.*, Radley Balko, *Another Week, Another Crime Lab Scandal*, WASH. POST (Oct. 20, 2017), https://www.washingtonpost.com/news/the-watch/wp/2017/10/20/another-week-another-crime-lab-scandal/ [https://perma.cc/7N7K-3WRR] (discussing the firing of a Massachusetts state crime lab head supervisor after it was revealed that lab staff withheld exculpatory evidence in thousands of drunk driving cases involving breathalyzer machines).

[136] Roth, *supra* note 27, at 1991 (internal quotation marks omitted).

[137] *See, e.g.*, Dave Gershgorn, *Facebook Built an AI System that Learned to Lie to Get What It Wants*, QUARTZ (June 14, 2017), https://qz.com/1004070/facebook-fb-built-an-ai-system-that-learned-to-lie-to-get-what-it-wants/ [https://perma.cc/86ZB-TB5A] (describing a Facebook artificial intelligence negotiating program: [T]he AI system didn't

machine testimony is fallible. Its operators might unintentionally bias its output even despite the overarching entity's efforts to avoid that via "multiple layers of scrutiny" in place as a safeguard.[138] Design errors of many sorts might cause the program to fail.[139] Just as these errors can be fatal outside the courtroom,[140] they can be in the courtroom as well.

For these reasons and others, the protections offered by the FRE are invaluable for criminal defendants facing machine accusers. Courts must apply them more rigorously. Doing so will also help address some related concerns for machine-generated testimony. For example, another commentator summarized many such dangers under the umbrella term "black box dangers":

> Just as human sources potentially suffer the so-called "hearsay dangers" of insincerity, ambiguity, memory loss, and misperception, machine sources potentially suffer "black box" dangers that could lead a factfinder to draw the wrong inference from information conveyed by a machine source. A machine does not exhibit a character for dishonesty or suffer from memory loss. But a machine's programming, whether the result of human coding or machine learning, could cause it to utter a falsehood by design. A machine's output could be imprecise or ambiguous because of human error at the programming,

---

only learn how to state its demands, but negotiation tactics as well—specifically, lying. Instead of outright saying what it wanted, sometimes the AI would feign interest in a worthless object, only to later concede it for something that it really wanted. Facebook isn't sure whether it learned from the human hagglers or whether it stumbled upon the trick accidentally, but either way when the tactic worked, it was rewarded.); *see also* Megan Geuss, *Volkswagen's Emissions Cheating Scandal Had a Long, Complicated History*, ARSTECHNICA (Sept. 24, 2017), https://arstechnica.com/cars/2017/09/volkswagens-emissions-cheating-scandal-has-a-long-complicated-history/ [https://perma.cc/CV52-ZSAL] (describing VW's and Audi's "software that allowed the cars to cheat on their US federal emissions tests").

[138] *See, e.g.*, Mike Isaac, *Facebook Trending List Skewed by Individual Judgment, Not Institutional Bias*, N.Y. TIMES (May 20, 2016), https://www.nytimes.com/2016/05/21/technology/facebook-trending-list-skewed-by-individual-judgment-not-institutional-bias.html [https://perma.cc/D87X-WZCD].

[139] *See, e.g.*, David Murray, *Queensland Authorities Confirm 'Miscode' Affects DNA Evidence In Criminal Cases*, THE COURIER-MAIL (Mar. 20, 2015), http://www.couriermail.com.au/news/queensland/queensland-authorities-confirm-miscode-affects-dna-evidence-in-criminal-cases/news-story/833c580d3f1c59039efd1a2ef55af92b [https://perma.cc/N2DK-N6D9].

[140] *See, e.g.*, David Shepardson, *Tesla Mulling Two Theories to Explain 'Autopilot' Crash: Source*, REUTERS (July 29, 2016), https://www.reuters.com/article/us-tesla-autopilot-congress-idUSKCN10928F [https://perma.cc/Y7EB-N7SC].

> input, or operation stage, or because of machine error due to degradation and environmental forces. And human and machine errors at any of these stages could also lead a machine to misanalyze an event. Just as the "hearsay dangers" are believed more likely to arise and remain undetected when the human source is not subject to the oath, physical confrontation, and cross-examination, black box dangers are more likely to arise and remain undetected when a machine utterance is the output of an "inscrutable black box."[141]

Thus, a critical right for defendants is the ability to challenge, through cross-examination of the individual(s) who ran the test, whether the defendant's actual sample was tested and tested properly. That adjustment, which is arguably required even under existing rules, will help address authentication issues, hearsay concerns, and many of the "black box" concerns above. In many criminal cases, the most compelling evidence is the lab's findings. Numerous false convictions have involved such evidence for just that reason—forensic evidence has tremendous power. After hundreds of lab scandals and tens of thousands of cases impacted (or even dismissed), courts should require more machine operators to testify in court. This will not prevent all such errors or fabrications, but it will prevent some. And requiring machine operators to testify will better protect defendants against errant or misled machine accusers. And if, for example, requiring more machine operators to testify averted just the Dookhan scandal, the requirement would have protected countless defendants and prevented a cloud of doubt cast over twenty thousand cases.[142]

CONCLUSION

Many courts have held that the rules of evidence are the proper tool to protect a defendant's rights as to machine testimony. If they are to carry that mantle, courts must apply them more faithfully. The alternatives—revising the FRE or reinterpreting the Confrontation

---

[141] Roth, *supra* note 27, at 1977–78 (internal footnotes and citations omitted). *But see* Stephen A. Saltzburg, *Equipment, Hearsay, and Authentication*, 22 CRIM. JUST. 38, 41 (2008) (arguing the absence of Confrontation Clause or hearsay problems and that authentication is sufficient on bases other than actual testing analyst's testimony).

[142] *See* Mettler, *supra* note 133 (describing a Massachusetts forensic analyst who falsified results by "not actually testing all the drugs that came before her, forging her co-workers' initials[,] and mixing drug samples so that her shoddy analysis matched the results she gave prosecutors," leading to the dismissal of 21,587 drug cases "tainted by [her] misconduct").

Clause—are much more difficult to achieve. Fortunately, the existing rules of evidence already provide avenues to help address the reliability and "black box" concerns described above.

For example, courts should subject machine accuser testimony to the requirements of the FRE hearsay provisions when the statement is the product of an operator exercising control over the machine accuser. The judiciary's current path of exempting nearly all machine statements is disingenuous and fails to reflect the reality that, in many situations, human operators control and thus contribute to the resulting machine accusation. In such an approach, courts would not apply the hearsay rules to the machine's role: for example, judges would not ponder if a machine could make a dying declaration when its batteries were low. Instead, courts would subject the human operator to hearsay analysis and, absent some exemption, the operator would often be required to testify. Similarly, courts generally should not find that machine accuser evidence is adequately authenticated if the individual(s) with first-hand knowledge of the tests do not testify. As with the hearsay analysis, this approach would lead to more machine operators testifying in court.

These or other analytical changes—such as reinterpreting the Confrontation Clause—are increasingly important as machine accusers aided by human operators rise in prevalence. Calling machine operators to testify would empower a defendant to examine whether his or her sample was tested properly. It would be excusable to believe, initially, that such basic matters as whether an analyst falsified results or ran the tests at all were not questions of any pertinence in the modern criminal justice system. But the stream of lab scandals described above erases any such notion. Again, errors of these sorts have occurred in more than a hundred domestic labs and have led to the dismissal of thousands of cases.[143] Thus, defendants should be empowered to inquire into whether the operator used the machine correctly,[144] otherwise erred in the analysis,[145] falsified results,[146] and actually ran any test whatsoever.[147] That can be accomplished in many cases by requiring machine operators to testify in court.

This will require some labs to restructure how tests are conducted to avoid the expense of producing numerous analysts to authenticate evidence.[148] However, if courts adopt this approach to the FRE, that does

[143] *See, e.g.*, sources cited *supra* note 134 (describing this issue).
[144] *See, e.g.*, Lindell, *supra* note 126 (describing this issue).
[145] *See, e.g.*, sources cited *supra* note 132 (describing this issue).
[146] *See, e.g.*, Lindell, *supra* note 126 (describing this issue).
[147] *See, e.g.*, sources cited *supra* note 133 (describing this issue).
[148] *See, e.g.*, Melendez-Diaz v. Massachusetts, 557 U.S. 305, 332–33 (2009) (Kennedy, J., dissenting) (discussing the various individuals involved in forensic drug analysis and

not foreclose statutory schemes that are designed to alleviate the burden on forensic labs: for example, rules that require the defendant to assert this right by a certain stage of trial to avoid its being deemed waived. Labs may also be able to adopt systems that reduce the number of individuals needed to testify. Even if they cannot, however, the difficulties faced under this analysis are dwarfed by years of analyst errors and falsification. This reality was brought about not just by the rules of evidence but also by the failure of forensic professionals to police their own to protect innocent defendants.

The argument that courts should more faithfully apply the authentication and hearsay rules does not suggest the absence of other ways to enhance the rules of evidence and the criminal system in general. For example, since many cases never go to trial, pre-trial disclosure is immensely valuable. Another alternative is modifying reliability rules that apply to scientific or technical methods of expert witnesses such that they also apply to machine-generated testimony. Applying *Daubert*- and *Frye*-style analysis to machine assertions could be one way to do so.[149] But, as another commentator has noted, that approach has proven fallible: in one case, "two expert DNA systems . . . came to . . . different conclusion[s, but] have both been accepted in numerous jurisdictions under both *Daubert* and *Frye*. These basic reliability tests, unless modified to more robustly scrutinize the software, simply do not—on their own—offer the jury enough context to choose the more credible system."[150]

In any event, the FRE should not bear this weight alone. As argued previously, the Confrontation Clause has a clear role to play as to data generated by a machine (and as to testimonial assertions courts have let slip in under the guise of machine-generated evidence, such as the assertion that a given lab report actually pertains to the defendant's biological sample). Additional government or industry regulation of, for example, forensic machines, could be helpful,[151] but it is not alone sufficient. Just as reliability was neither the touchstone nor constitutionally sufficient in *Crawford*, so too is regulation an inadequate substitute for what the Constitution commands: the right to confront one's accusers. The

---

arguing that a rule requiring calling all of them to testify "for all practical purposes, forbid[s] the use of scientific results in criminal trials").

[149] *Cf.* Roth, *supra* note 27, at 2032–33 (making this same argument but also suggesting a distinction between "lay observations" such as those "of a poorly programmed robot security guard" and machine "conveyances [that] relate to matters beyond the ken of the jury").

[150] *Id.* at 2035.

[151] *See, e.g.*, *id.* at 2023–26 (discussing "front-end design, input, and operation protocols" such as "requir[ing] any software-driven system used in litigation to be certified as having followed software industry standards in design and testing").

Confrontation Clause should empower defendants to confront machine accusers just as it empowered defendants to confront the human accusers the machines replaced.

This article focused largely on the dangers inherent in machines built by humans and operated by human agents—agents who can err or intentionally mislead the machine's analysis or assertions. It reduced that field of machines to the even narrower range of machine accusers that are operated by analysts who exercise control over the accusation. But as machines grow increasingly complex, the judicial system must be prepared to account for machines that are fully autonomous—and potentially even machines that learn to lie. Such quandaries are neither science fiction nor prediction; they have, in limited contexts, happened already.[152] This is an issue that is going to get worse, not better. As machines increasingly assume the roles once occupied by humans, more and more criminal accusers will be immune to the crucible of cross-examination. *Someone* might testify in court, but as the cases described herein demonstrate, that individual might lack any first-hand knowledge of the accusation's basis. Just as breathalyzer-style machines evolved from creating results requiring human assistance to producing automated print-outs, so too will existing machines increasingly stand on their own feet.[153] When the prosecution fills its evidence list with machine accusers and their human supervisors—supervisors who have no first-hand knowledge of the analysis allegedly conducted—how will the defendant prove the machine erred or was influenced to err? The hardest decisions are ahead of us, not behind, and they are decisions that courts will be forced to adjudicate soon. If technology continues at its usual pace, "soon" will be upon us earlier than we think.

[152] *See, e.g.*, Sara Mitri et al., *The Evolution of Information Suppression in Communicating Robots with Conflicting Interests*, 106 PROC. NAT'L ACAD. SCI. 15786, 15787–88 (2009) (describing robots that learned to suppress information that could lead other robots to find food).

[153] *See, e.g.*, Roth, *supra* note 27, at 2016 (making this observation as to breathalyzers and other machine witnesses).