THE YALE LAW JOURNAL

Machine Testimony

ANDREA ROTH

ABSTRACT. Machines play increasingly crucial roles in establishing facts in legal disputes. Some machines convey information—the images of cameras, the measurements of thermometers, the opinions of expert systems. When a litigant offers a human assertion for its truth, the law subjects it to testimonial safeguards—such as impeachment and the hearsay rule—to give juries the context necessary to assess the source's credibility. But the law on machine conveyance is confused: courts shoehorn them into existing rules by treating them as "hearsay," as "real evidence," or as "methods" underlying human expert opinions. These attempts have not been wholly unsuccessful, but they are intellectually incoherent and fail to fully empower juries to assess machine credibility. This Article seeks to resolve this confusion and offer a coherent framework for conceptualizing and regulating machine evidence. First, it explains that some machine evidence, like human testimony, depends on the credibility of a source. Just as so-called "hearsay dangers" lurk in human assertions, "black box dangers"—human and machine errors causing a machine to be false by design, inarticulate, or analytically unsound—potentially lurk in machine conveyances. Second, it offers a taxonomy of machine evidence, explaining which types implicate credibility and how courts have attempted to regulate them through existing law. Third, it offers a new vision of testimonial safeguards for machines. It explores credibility testing in the form of front-end design, input, and operation protocols; pretrial disclosure and access rules; authentication and reliability rules; impeachment and courtroom testing mechanisms; jury instructions; and corroboration rules. And it explains why machine sources can be "witnesses" under the Sixth Amendment, refocusing the right of confrontation on meaningful impeachment. The Article concludes by suggesting how the decoupling of credibility testing from the prevailing courtroom-centered hearsay model could benefit the law of testimony more broadly.

AUTHOR. Assistant Professor of Law, UC Berkeley School of Law. The author wishes to thank George Fisher, Erin Murphy, Daniel Richman, David Sklansky, and Eleanor Swift for extensive feedback. For technical information I am grateful to Nathaniel Adams, Jennifer Friedman, Angelyn Gates, Jessica Goldthwaite, Andrew Grosso, Allan Jamieson, Dan Krane, and Terri Rosenblatt. I am also indebted to Ty Alper, Laura Appleman, David Ball, Ryan Calo, Edward Cheng, Catherine Crump, David Engstrom, Dan Farber, Brandon Garrett, Andrew Gilden, Robert Glushko, Chris Hoofnagle, Edward Imwinkelried, Elizabeth Joh, Owen Jones, Robert MacCoun, Jennifer Mnookin, Deirdre Mulligan, Melissa Murray, John Paul Reichmuth, Pamela Samuelson, Jonathan Simon, Aaron Simowitz, Christopher Slobogin, Avani Mehta Sood, Rachel Stern, Karen Tani, Kate Weisburd, Charles Weisselberg, Rebecca Wexler, Tal Zarsky, the Berkeley Law junior faculty, and participants in the Berkeley, Stanford, Vanderbilt, and Willamette faculty workshops. Christian Chessman, Jeremy Isard, Purba Mukerjee, and Allee Rosenmayer offered excellent research assistance, and the *Yale Law Journal* editors offered invaluable editorial guidance.

ARTICLE CONTENTS

INTRODUCTION

In 2003, Paciano Lizarraga-Tirado was arrested and charged with illegally reentering the United States after having been deported.[1] He admitted that he was arrested in a remote area near the United States-Mexico border, but claimed he was arrested in Mexico while awaiting instructions from a smuggler. To prove the arrest occurred in the United States, the prosecution offered the testimony of the arresting officers that they were familiar with the area and believed they were north of the border, in the United States, when they made the arrest. An officer also testified that she used a Global Positioning System (GPS) device to determine their location by satellite, and then inputted the coordinates into Google Earth. Google Earth then placed a digital "tack" on a map, labeled with the coordinates, indicating that the location lay north of the border.[2] Mr. Lizarraga-Tirado insisted that these mechanical accusations were "hearsay," out-of-court assertions offered for their truth, and thus inadmissible. The Ninth Circuit rejected his argument, even while acknowledging that the digital "tack" was a "clear assertion[]," such that if the tack had been manually placed on the map by a person, it would be "classic hearsay."[3] In the court's view, machine assertions—although raising reliability concerns[4]—are simply the products of mechanical processes and, therefore, akin to physical evidence. As such, they are adequately "addressed by the rules of authentication," requiring the proponent to prove "that the evidence 'is what the proponent claims it is,'"[5] or by "judicial notice,"[6] allowing judges to declare the accuracy of certain evidence by fiat.

Mr. Lizarraga-Tirado's case is emblematic of litigants' increasing reliance on information conveyed by machines.[7] While scientific instruments and cameras have been a mainstay in courtrooms for well over a century, the past century has witnessed a noteworthy rise in the "'silent testimony' of instruments."[8] By

1. United States v. Lizarraga-Tirado, 789 F.3d 1107, 1108 (9th Cir. 2015).
2. *Id.*
3. *Id.* at 1109.
4. *Id.* at 1110; *see also* MICHAEL HARRINGTON & MICHAEL CROSS, GOOGLE EARTH FORENSICS: USING GOOGLE EARTH GEO-LOCATION IN DIGITAL FORENSIC INVESTIGATIONS 40 (2015) (noting potential errors in GPS signaling).
5. *Lizarraga-Tirado*, 789 F.3d at 1110 (quoting FED. R. EVID. 901(a)).
6. *Id.*
7. By "machine," I mean an artificial apparatus designed to perform a task.
8. MIRJAN R. DAMAŠKA, EVIDENCE LAW ADRIFT 143 (1997).

the 1940s, courts had grappled with "scientific gadgets" such as blood tests and the "Drunk-O-Meter,"[9] and by the 1960s, the output of commercially used tabulating machines.[10] Courts now routinely admit the conveyances[11] of complex proprietary algorithms, some created specifically for litigation, from infrared breath-alcohol-testing software to expert systems diagnosing illness or interpreting DNA mixtures. Even discussions of the potential for robot witnesses have begun in earnest.[12]

This shift from human- to machine-generated proof has, on the whole, enhanced accuracy and objectivity in fact finding.[13] But as machines extend their reach and expertise, to the point where competing expert systems have reached different "opinions" related to the same scientific evidence,[14] a new sense of urgency surrounds basic questions about what machine conveyances are and what problems they pose for the law of evidence. While a handful of scholars have suggested in passing that "the reports of a mechanical observer" might be

9. *See, e.g.*, Dillard S. Gardner, *Breath-Tests for Alcohol: A Sampling Study of Mechanical Evidence*, 31 TEX. L. REV. 289, 289 (1953); *Notes and Legislation—Scientific Gadgets in the Law of Evidence*, 53 HARV. L. REV. 285, 285 (1939).

10. *See* discussion *infra* Section II.B.3.

11. I use the term "machine conveyance" to capture machine output that conveys information. I avoid the term "machine assertion" because "assertion" in the hearsay context denotes a statement by a declarant having assertive "inten[t]." *See, e.g.*, FED. R. EVID. 801(a). Nonetheless, a lively debate surrounds whether machines might be capable of cognition and intentional behavior. *See* discussion *infra* Section I.A.

12. *See* discussion *infra* Section II.B.5.

13. *See generally* Andrea Roth, *Trial by Machine*, 104 GEO. L.J. 1245 (2016) (documenting the rise of mechanical proof and decision making in criminal trials as a means of enhancing objectivity and accuracy, at least when the shift toward the mechanical has benefitted certain interests).

14. *See infra* notes 249-256 and accompanying text.

assertive claims implicating credibility,[15] legal scholars have not yet explored machine conveyances in depth.[16]

This Article seeks to resolve this doctrinal and conceptual confusion about machine evidence by making three contributions. First, the Article contends that some types of machine evidence merit treatment as credibility-dependent conveyances of information. Accordingly, the Article offers a framework for understanding machine credibility by describing the potential infirmities of machine sources. Just as human sources potentially suffer the so-called "hearsay dangers" of insincerity, ambiguity, memory loss, and misperception,[17] machine sources potentially suffer "black box" dangers[18] 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 cod-

15. Richard D. Friedman, *Route Analysis of Credibility and Hearsay*, 96 YALE L.J. 667, 673-74 n.17 (1987) (noting that "non-human witnesses" could include "mechanical observer[s]" like thermometers and radar guns); *see also* David A. Schum, *Hearsay from a Layperson*, 14 CARDOZO L. REV. 1, 2-3 (1992) (acknowledging that "mechanical devices" could be potential "sources in a hearsay chain"); Jessica M. Silbey, *Judges as Film Critics: New Approaches to Filmic Evidence*, 37 U. MICH. J.L. REFORM 493, 508 n.62 (2004) (arguing that filmic evidence is "testimonial in nature"); *cf.* Ernest Sosa, *Knowledge: Instrumental and Testimonial*, *in* THE EPISTEMOLOGY OF TESTIMONY 116, 116-17 (Jennifer Lackey & Ernest Sosa eds., 2006) (positing that "[t]estimonial knowledge" is "closely related" to the "instrumental" knowledge offered by "[a] deliverance of a proposition by an instrument").

16. While this Article is the first to explore machine assertions systematically as credibility-dependent proof, other legal commentators have recognized the need to probe machines' inner workings given the increasing reliance on machines in litigation. *See, e.g.*, Edward J. Imwinkelried, *Computer Source Code: A Source of the Growing Controversy over the Reliability of Automated Forensic Techniques* (UC Davis Legal Studies Research Paper Series, Research Paper No. 487, 2016), http://ssrn.com/abstract=2764593 [http://perma.cc/G74K-ZVL7]; Christian Chessman, Note, *A "Source" of Error: Computer Code, Criminal Defendants, and the Constitution*, 105 CALIF. L. REV. 101 (forthcoming 2017). One scholar has also examined how existing Confrontation Clause jurisprudence applies to machine-generated data. *See* Brian Sites, *Rise of the Machines: Machine-Generated Data and the Confrontation Clause*, 16 COLUM. SCI. & TECH. L. REV. 36, 99-100 (2014).

17. *See, e.g.*, Edmund M. Morgan, *Hearsay Dangers and the Application of the Hearsay Concept*, 62 HARV. L. REV. 177 (1948).

18. Numerous writers in the technology space have used the "black box" language to describe inscrutable algorithmic processes. *See, e.g.*, NICHOLAS CARR, THE GLASS CAGE: AUTOMATION AND US 163 (2014); FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015).

ing or machine learning,[19] 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, 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,[20] black box dangers are more likely to arise and remain undetected when a machine utterance is the output of an "inscrutable black box."[21]

Because human design, input, and operation are integral to a machine's credibility, some courts and scholars have reasoned that a human is the true "declarant"[22] of any machine conveyance.[23] But while a designer or operator might be partially epistemically or morally responsible for a machine's statements, the human is not the sole source of the claim. Just as the opinion of a human expert is the result of "distributed cognition"[24] between the expert and her many lay and expert influences,[25] the conveyance of a machine is the result of "distribut[ed] cognition between technology and humans."[26] The machine is

19. "Machine learning" systems are "computer algorithms that have the ability to 'learn' or improve in performance over time on some task." Harry Surden, *Machine Learning and Law*, 89 WASH. L. REV. 87, 88 (2014).

20. Of course, the term "hearsay dangers" is itself misleading; these infirmities potentially lurk in all human testimony, not just out-of-court "hearsay." And the courtroom safeguards promoted by the hearsay rule are not the only, or even necessarily the most effective, means of testing human credibility in some contexts. *See* discussion *infra* Section I.A.

21. CARR, *supra* note 18, at 163.

22. "Declarant" is a term used in the hearsay context to label the person making the assertion offered for its truth. For clarity, this Article uses the term "source" to refer broadly to any source conveying a claim, offered for its truth, in a way that implicates the source's credibility.

23. *See, e.g.*, Jianniney v. State, 962 A.2d 229, 232 (Del. 2008) (excluding Mapquest driving estimates as inadmissible hearsay); Adam Wolfson, Note, *"Electronic Fingerprints": Doing Away with the Conception of Computer-Generated Records as Hearsay*, 104 MICH. L. REV. 151, 155-56 (2005) (noting courts' tendencies to treat machine-generated data as hearsay); *see also* discussion *infra* Section I.A.

24. Itiel E. Dror & Jennifer L. Mnookin, *The Use of Technology in Human Expert Domains: Challenges and Risks Arising from the Use of Automated Fingerprint Identification Systems in Forensic Science*, 9 LAW PROBABILITY & RISK 1, 2 (2010).

25. In the software context, there may be numerous collaborating programmers rather than one human epistemic source. I thank Mona Pinchis for this point.

26. Dror & Mnookin, *supra* note 24, at 1.

influenced by others, but is still a source whose credibility is at issue. Thus, any rule requiring a designer, inputter, or operator to take the stand as a condition of admitting a machine conveyance should be justified based on the inability of jurors, without such testimony, to assess the black box dangers. In some cases, human testimony might be unnecessary or, depending on the machine, insufficient to provide the jury with enough context to draw the right inference. Human experts often act as "mere scrivener[s]"[27] on the witness stand, regurgitating the conveyances of machines. Their testimony might create a veneer of scrutiny when in fact the actual source of the information, the machine, remains largely unscrutinized.

Second, the Article offers a taxonomy of machine evidence that explains which types implicate credibility and explores how courts have attempted to regulate them. Not all machine evidence implicates black box dangers. Some machines are simply conduits for the assertions of others, tools facilitating testing, or conveyances offered for a purpose other than truth. But "silent witnesses" that convey images and machines that convey symbolic output—from pendulum clocks to probabilistic genotyping software—do implicate black box dangers. These claim-conveying machines vary widely in their complexity, opacity, sensitivity to case-specific human manipulation, and litigative or nonlitigative purpose, and they might involve a low or high risk of inferential error absent a further opening of their black box. But they should be recognized, in the first instance, as credibility-dependent proof. As it turns out, courts have often shown promising intuitions about black box dangers in their attempts to regulate machine conveyances. But those attempts, particularly with respect to proprietary algorithms created for litigation, have too often been incoherent or incomplete. Meanwhile, commentators sometimes conflate credibility-dependent machine evidence with machine tools, conduits, or conveyances offered for a purpose other than truth when describing the influx of machine evidence into criminal trials.[28]

---

27. *See* Bullcoming v. New Mexico, 564 U.S. 647, 672 (2011) (Sotomayor, J., concurring) (quoting State v. Bullcoming, 226 P.3d 1, 9 (N.M. 2010)).

28. *See, e.g.*, Alex Hern & Sam Thielman, *Amazon Refuses To Let Police Access US Murder Suspect's Echo Recordings*, GUARDIAN (Dec. 28, 2016), http://www.theguardian.com/technology/2016/dec/28/amazon-refuses-to-let-police-access-suspects-echo-recordings [http://perma.cc/AYD6-3MTC] (describing issues related to the rise of prosecutorial use of "'smart' device data," and implicitly analogizing Echo data, which simply records human voices, to Fitbit data, which actually perceives human biological phenomena and digitally reports its algorithm-based calculations).

Finally, the Article offers a new vision of testimonial safeguards for machine sources of information. For several reasons, the Article does not advocate a broad rule of exclusion, akin to the hearsay rule, for "risky" machines.[29] First, the hearsay rule itself could not easily be modified to accommodate machines, given its focus on the oath, physical confrontation, and cross-examination. Second, a broad category of exclusion might be less appropriate for machine sources than for human sources, whose frailties and foibles largely motivated the rise of machine-generated proof to begin with.[30] Third, even with respect to human declarants, the hearsay rule is already highly unpopular for categorically excluding so much relevant evidence while being riddled with exceptions that are largely tradition-based and empirically unfounded.[31] Instead, this Article focuses on safeguards that would offer the jury key foundational facts or context[32] to better assess the accuracy[33] of machine conveyances.

Lawmakers should first consider design, input, and operation protocols to improve accuracy, much like the protocols that govern breath-alcohol machines and, in some states, eyewitness testimony.[34] Such front-end protocols could include software testing, machine-learning performance evaluations, and variations of "adversarial design,"[35] in which competing perspectives are incorporated at the design stage into the variables and analytical assumptions of

29. *See* Eleanor Swift, *Abolishing the Hearsay Rule*, 75 CALIF. L. REV. 495, 518 (1987) (arguing that the hearsay rule's primary value, if any, is in excluding "[r]isky," "[a]bstract," or "[b]urden-[s]hifting" declarants whose assertions would otherwise be admitted absent the rule).

30. *See, e.g.*, Tal Z. Zarsky, *Automated Prediction: Perception, Law, and Policy*, 15 COMMS. ACM 33, 34 (2012) (arguing that automated prediction "actually *promotes* important social objectives" by offering objectivity and fairness lacking in human review).

31. *See* discussion *infra* at Section III.A.3.

32. *See generally* Eleanor Swift, *A Foundation Fact Approach to Hearsay*, 75 CALIF. L. REV. 1339 (1987) (arguing for an approach to hearsay that focuses on giving factfinders sufficient context about a statement's meaning, rather than on excluding unreliable assertions).

33. By "accuracy," I mean the various ways in which a machine conveyance's result actually corresponds to empirical reality, whether by avoiding false positives (high specificity) or false negatives (high sensitivity). A machine might also be well "calibrated" in the sense that it is not over- or underconfident in its probability assessments – i.e., that its expression of the uncertainty inherent in its assessment is itself accurate. *See* Robert J. MacCoun, *The Epistemic Contract: Fostering an Appropriate Level of Public Trust in Experts*, *in* MOTIVATING COOPERATION AND COMPLIANCE WITH AUTHORITY: THE ROLE OF INSTITUTIONAL TRUST 191, 200 (Brian H. Bornstein & Alan J. Tomkins eds., 2015).

34. *See* discussion *infra* Section III.A.1.

35. *See generally* CARL DISALVO, ADVERSARIAL DESIGN 1 (2012) (exploring the use of design in spaces and systems to enable "agonism," a paradigm of political contentiousness as a positive and appropriate force for change).

algorithms. Next, lawmakers should consider pretrial disclosure and access rules for machines, especially machine "experts." These rules might allow litigants to access machines before trial to test different parameters or inputs (much like posing hypotheticals to human experts). The rules might also require public access to programs for further testing or "tinkering";[36] disclosure of "source code,"[37] if necessary to meaningfully scrutinize the machine's claims;[38] and the discovery of prior statements or "Jencks material"[39] of machines, such as COBRA data for breath-testing machines.[40] Lawmakers should also continue to require authentication of machine-related items to ensure that a machine conveyance, whether a DNA-typing printout or email, is what the proponent says it is.[41]

For machines offering "expert" evidence on matters beyond the ken of the jury,[42] lawmakers should clarify and modify existing *Daubert* and *Frye* reliability requirements for expert methods[43] to ensure that machine processes are

---

36. Maayan Perel & Niva Elkin-Koren, *Black Box Tinkering: Beyond Transparency in Algorithmic Enforcement*, 69 FLA. L. REV. (forthcoming 2017).

37. "Source code" is written in "human-readable language," and then compiled into executable machine code, which directly instructs the computer running the program. *See* People v. Superior Court *ex rel.* Chubbs, No. B258569, 2015 WL 139069, at *7 (Cal. Ct. App. Jan. 9, 2015).

38. *See* discussion *infra* Section III.A.2.

39. *Cf.* 18 U.S.C. § 3500(b) (2012) (requiring disclosure of certain prior statements of witnesses in criminal cases).

40. *See, e.g.*, Kathleen E. Watson, Note, *COBRA Data and the Right To Confront Technology Against You*, 42 N. KY. L. REV. 375, 381 (2015) ("In order to produce reasonable doubt as to the validity of a breath test result, the defense expert witness must have access to COBRA data. Without it, interrogation and cross-examination regarding the accuracy and reliability of a specific breath test is exceedingly limited.").

41. Authentication rules, by requiring proof that an item is what it purports to be, seek to ensure an item's *relevance*, not its *reliability*. While Federal Rule of Evidence 901(b)(9) allows authentication of results of a "process or system" by showing the system produces an "accurate result," this provision is not an accuracy requirement and, in any event, was a sui generis rule created in 1968 to accommodate computerized business records. *See* discussion *infra* Sections II.B.3, III.A.3.

42. *See, e.g.*, FED. R. EVID. 702(a) advisory committee's note to 1972 proposed rules. Some machines, such as robot security guards, will offer the equivalent of lay testimony. *See* discussion *infra* Section III.A.3.

43. *See* Daubert v. Merrell Dow Pharm., Inc., 509 U.S. 579, 579-80 (1993) (requiring judges to determine that scientific or technical methods underlying expert testimony be scientifically valid); Frye v. United States, 293 F. 1013, 1014 (D.C. Cir. 1923) (holding that novel scientific methods must "have gained general acceptance in the particular field in which [they] belong[]").

based on reliable methods and are implemented in a reliable way. *Daubert-Frye* hearings are a promising means of excluding the most demonstrably unreliable machine sources, but beyond the obvious cases, these hearings do not offer sufficient scrutiny. Judges generally admit such proof so long as validation studies can demonstrate that the machine's error rate is low and that the principles underlying its methodology are sound.[44] But validation studies are often conducted under idealized conditions, and it is precisely in cases involving less-than-ideal conditions—degraded or highly complex mixtures difficult for human analysts to interpret—that expert systems are most often deployed and merit the most scrutiny. Moreover, machine conveyances are often in the form of predictive scores and match statistics, which are harder to falsify through validation against a known baseline. For example, even if a DNA expert system rarely falsely includes a suspect as a contributor to a DNA mixture, its match statistics might be off by orders of magnitude because of a host of human or machine errors, potentially causing jurors to draw the wrong inference. Courts applying *Daubert-Frye* to software-generated statements should treat software engineers as part of the relevant scientific community and determine reliability not only of the method, but also of the software implementing that method, based on industry standards. In some cases, courts would likely need to access proprietary source code to assess the code's ability to operationalize an otherwise reliable method.

Beyond the admissibility stage, an opponent should be allowed to impeach machines at trial, just as the opponent can impeach human witnesses and declarants even when a judge deems their assertions reliable.[45] Lawmakers should allow impeachment of machines by inconsistency, incapacity, and the like, as well as by evidence of bias or bad character in human progenitors. Lawmakers might even impose live testimony requirements for human designers, inputters, or operators in certain cases where testimony is necessary to scrutinize the accuracy of inputs, as the United Kingdom has done in criminal cases. Courts could also give jury instructions for certain machines typically under- or overvalued by jurors, akin to those used for human declarants like accomplices. And they could impose corroboration requirements, akin to those imposed on accomplice testimony and confessions, for certain risky machines or machines whose results lie within a certain margin of error. Such requirements might be

44. *See* discussion *infra* Section III.A.3.

45. *See, e.g.*, FED. R. EVID. 806 (allowing impeachment of hearsay declarants).

grounded in concerns not only about accuracy, but also about public legitimacy in cases where the sole evidence of guilt is machine output.[46]

Finally, in criminal cases, machine sources of accusation—particularly proprietary software created for litigation—might be "witnesses against" a defendant under the Confrontation Clause.[47] Accusatory machine output potentially implicates the central concerns underlying the Clause in three ways. First, if substituted for the testimony of witnesses otherwise subject to credibility testing, machine testimony allows the State to evade responsibility for accusations. Second, the State's ability to shape and shield testimony from scrutiny through proprietary black box algorithms is analogous to the ex parte affidavit practice that preoccupied the Framers. Third, machines are potentially unreliable when their processes are shrouded in a black box. While machines generally cannot be physically confronted, they can be impeached in other ways, and courts and scholars should revisit cases in which the Supreme Court appears to recognize implicitly that "confrontation" includes a right of meaningful impeachment.

Part I of this Article argues that some machine evidence implicates credibility and catalogs black box dangers—potential testimonial infirmities of machine sources. Part II offers a taxonomy of machine evidence, explaining which types do and do not implicate credibility and exploring how courts have attempted to regulate different machine conveyances under existing law. Part III suggests testimonial safeguards for machines, including both credibility-testing mechanisms that would target the black box dangers and methods of confronting accusatory machine conveyances under the Sixth Amendment. The Article concludes by explaining how the law of testimony more broadly could be improved by decoupling credibility testing and the hearsay rule and refocusing safeguards for all testimony on a right of meaningful impeachment.

I. A FRAMEWORK FOR IDENTIFYING CREDIBILITY-DEPENDENT MACHINE EVIDENCE

This Part argues that some machine evidence implicates the credibility of its machine source—that is, the machine's worthiness of being believed. It then offers a framework for describing the testimonial infirmities of machines, cataloging the black box dangers of falsehood by design, inarticulateness, and ana-

46. *See* discussion *infra* Section III.A.5.

47. One scholar—in arguing that the Clause does not cover most machine-generated data—has suggested that the Clause might "evolve" to include machines. *See* Sites, *supra* note 16, at 99-100.

lytical error—caused by a variety of human and machine errors at the design, input, and operation stages—that might cause a factfinder to draw an improper inference from a machine source of information.

A. Machines as Sources Potentially in Need of Credibility Testing

How testimony[48] differs from alternative ways we come to know facts has been the subject of debate. Epistemologists generally recognize a distinction between "testimony" and "non-informational expressions of thought."[49] Legal scholars have also suggested a distinction between "testimony" and other evidence. Nineteenth-century treatise writer Thomas Starkie described "testimony" as "information derived . . . from those who had actual knowledge of the fact,"[50] and physical evidence as objects or conduct capable of being assessed through "actual and personal observation" by the jury.[51]

Both physical and testimonial evidence can lead to decisional inaccuracy. A jury asked to draw inferences from physical evidence, such as a large blood-stained serrated knife allegedly found in the defendant's purse after the murder, must be given the tools to determine that the large blood-stained serrated knife is, in fact, the same knife that was found in the defendant's purse. This process of "authenticating" the knife might require testimony of witnesses who found the knife, and that testimony might have its own set of credibility problems. But factfinders can assess, based on their own powers of observation and reasoning, the probative value of the knife's physical properties.

Testimonial evidence presents different challenges for decisional accuracy. Even if the factfinder's powers of observation and inference are working well, she might draw an improper inference if the source is not worthy of belief. In the hopes of offering juries sufficient context to assess the probative value of

---

48. "Testimony," broadly speaking, means the "reports of others." Jennifer Lackey, *Introduction* to THE EPISTEMOLOGY OF TESTIMONY 1 (Jennifer Lackey & Ernest Sosa eds., 2006).

49. *Id.* at 2 (emphasis omitted).

50. 1 JOHN HENRY WIGMORE, A TREATISE ON THE ANGLO-AMERICAN SYSTEM OF EVIDENCE IN TRIALS AT COMMON LAW § 25, at 224-25 (2d ed. 1923) (citing 1 THOMAS STARKIE, LAW OF EVIDENCE § 13 (1824)).

51. *Id.*; *see also* SIMON GREENLEAF, A TREATISE ON THE LAW OF EVIDENCE § 13, at 16 (Gaunt, Inc. photo. reprt. 1997) (1st ed. 1842) (describing facts as either "directly attested by those, who speak with their own actual and personal knowledge of its existence," or "inferred from other facts, satisfactorily proved").

human testimony,[52] American jurisdictions have adopted rules of exclusion,[53] disclosure,[54] impeachment,[55] and corroboration,[56] and, to a lesser extent, jury instructions[57] and rules of production,[58] to screen out the most egregiously noncredible human sources and—if testimony is admitted—to empower fact-finders with information sufficient for them to assess accurately a source's credibility.

Predictably, lawmakers and scholars disagree about precisely which human acts and utterances should be subject to these safeguards. But they all invoke the same potential infirmities—the so-called "hearsay dangers"—of human sources: insincerity, inarticulateness, erroneous memory, and faulty perception.[59] For example, scholars seem to agree that so-called "implied assertions"—acts and utterances not intended by the source as an assertion, but that convey the source's belief that a condition is true and are offered to prove the truth of that belief—trigger credibility concerns because their probative value turns on the source's perceptive abilities.[60] But courts generally exempt "im-

52. *See* ALEX STEIN, FOUNDATIONS OF EVIDENCE LAW 8, 23 (2005) (discussing evidence law's focus as being the pursuit of decisional accuracy).

53. *See, e.g.*, FED. R. EVID. 802 (generally excluding hearsay); *id.* at 601-03 (laying out competence rules requiring an oath and personal knowledge).

54. *See, e.g.*, Jencks Act, 18 U.S.C. § 3500 (2012) (requiring disclosure of prior statements of testifying witnesses to facilitate impeachment at trial); FED. R. CRIM. P. 16(a)(1)(G) (requiring disclosure of the bases of an expert's opinion); *id.* at 26.2.

55. *See, e.g.*, FED. R. EVID. 609; *id.* at 801(d)(1)(A) (allowing impeachment by inconsistency).

56. *See, e.g.*, N.Y. CRIM. PROC. LAW § 60.22 (McKinney 2016) (prohibiting a criminal conviction "upon the testimony of an accomplice unsupported by corroborative evidence").

57. *See, e.g.*, "Testimony of an Accomplice," Ill. Crim. Jury Instr. 3.17 (warning jurors to view the testimony of an accomplice with "suspicion" and "with caution").

58. *See, e.g.*, State v. Henderson, 27 A.3d 872, 878 (N.J. 2011) (establishing protocols for eyewitness identification procedures).

59. *See, e.g.*, Morgan, *supra* note 17. The "inarticulateness" danger is sometimes called "ambiguity," Laurence H. Tribe, Comment, *Triangulating Hearsay*, 87 HARV. L. REV. 957, 959 (1974); problems with "use of language," Morgan, *supra* note 17, at 178; or problems with "narration," Roger C. Park, *"I Didn't Tell Them Anything About You": Implied Assertions as Hearsay Under the Federal Rules of Evidence*, 74 MINN. L. REV. 783, 785-86 & n.15 (1990).

60. *See, e.g.*, Park, *supra* note 59, at 788. I understand that some scholars would refuse to label such acts or utterances "assertions" because they are not intended to be assertive. Nonetheless, the term "implied assertion" endures. *See, e.g.*, FED. R. EVID. 801 advisory committee's note to 1972 proposed rules (citing Ted Finman, *Implied Assertions as Hearsay: Some Criticisms of the Uniform Rules of Evidence*, 14 STAN. L. REV. 682 (1962)); Park, *supra* note 59.

plied assertions" from the hearsay rule because other infirmities, such as insincerity, are unlikely to arise.[61]

Lawmakers and scholars should likewise be open to viewing machine acts and utterances as dependent on credibility, if their probative value turns on whether a machine suffers testimonial infirmities. A handful of scholars have acknowledged that a machine, if it conveys information relied upon by others, offers testimonial knowledge, or a type of "instrumental knowledge" "closely related" to testimonial knowledge.[62] A handful of courts have also used words like "credibility" and "impeachment" to describe machine sources.[63]

Two theoretical objections to the concept of "machine credibility" might be raised at the outset. The first is, as some courts and litigants have insisted, that machine conveyances are simply the hearsay assertions of the machine's human programmer or inputter.[64] This argument offers a strategic payoff for some litigants, particularly criminal defendants, as it would exclude the machine conveyance absent live testimony of the programmer. The argument also has intuitive appeal. Even the most sophisticated machines today are bundles of metal and circuitry whose journey from "on" switch to output begins with the instructions laid out for them; even robots "are not capable of deviating from the code that constitutes them."[65]

Ultimately, though, this argument fails. That a programmer has designed a machine to behold and report events does not mean the programmer herself has borne witness to those events. As the Fourth Circuit noted in rejecting such an argument with respect to a gas chromatograph, "[t]he technicians could neither have affirmed [n]or denied *independently* that the blood contained" drugs "because all the technicians could do was to refer to the raw data printed

---

61. *See, e.g.*, FED. R. EVID. 801 advisory committee's note to 1972 proposed rules.

62. Sosa, *supra* note 15, at 116.

63. *See* discussion *infra* Section III.A.4.

64. *See, e.g.*, United States v. Washington, 498 F.3d 225, 229 (4th Cir. 2007) (explaining defendant's argument that the "raw data" of a chromatograph was the "hearsay" of the "technicians" who tested the defendant's blood sample for PCP and alcohol using the machine); Karen Neville, *Programmers and Forensic Analyses: Accusers Under the Confrontation Clause*, 2011 DUKE L. & TECH. REV., no. 10, at 1, 9 (arguing that "the programmer" is "the 'true accuser'—not the machine merely following the protocols he created").

65. Ryan Calo, *Robots in American Law* 41 (Univ. of Wash. Sch. of Law, Legal Studies Research Paper No. 2016-04, 2016), http://ssrn.com/abstract=2737598 [http://perma.cc/ENA4-A3WL].

out by the machine."[66] The argument also fails to recognize the phenomenon of machine learning[67] and other unpredictable aspects of modern machine operation; "[p]rogrammers do not, and often cannot, predict what their complex programs will do."[68] Indeed, machine learning "can lead to solutions no human would have come to on her own," including patentable inventions[69] and award-winning literature.[70]

That is not to say that humans bear no responsibility for machine output. A programmer might be legally responsible for machine output that is socially harmful[71] or have output imputed to him under a fairness-based "opposing party admission"-type doctrine.[72] A programmer might also be partially epistemically responsible for machine output because she gives the machine its analytical parameters and instructions. In the human context, an expert witness's Ph.D. advisor, or witnesses interviewed by an expert in the course of rendering an expert opinion, might be partially epistemically responsible for the expert's opinions. Evidence scholars call this phenomenon "distributed

---

66. *Washington*, 498 F.3d at 230; *see also* People v. Goldsmith, 326 P.3d 239, 249 (Cal. 2014) (holding that red light time-stamp data was not the hearsay of the programmer, where no one was "present watching the intersection and deciding to take the photographs and video"); State v. Armstead, 432 So. 2d 837, 839-40 (La. 1983) (holding that the machine's statements were not "dependent upon the observations and reporting of a human declarant"); People v. Dinardo, 801 N.W.2d 73, 78-79 (Mich. Ct. App. 2010) (holding that a DataMaster breath-alcohol "ticket" was not the statement of a human because the ticket was "self-explanatory data produced entirely by a machine"); Wimbish v. Commonwealth, 658 S.E.2d 715, 719-20 (Va. Ct. App. 2008) ("[N]o human entered into the Intoxilyzer 5000 the conclusion that [the defendant's] breath alcohol content was .22 grams per 210 liters of breath. [The defendant] blew into the machine, the machine analyzed his breath and reported the results of its analysis. The machine was the sole source of the test results.").

67. *See generally* Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PA. L. REV. 871 (2016) (discussing machine learning in crime-detecting machine technologies).

68. Zeynep Tufekci, *The Real Bias Built in at Facebook*, N.Y. TIMES (May 19, 2016), http://www.nytimes.com/2016/05/19/opinion/the-real-bias-built-in-at-facebook.html [http://perma.cc/Z6MC-DRLU].

69. Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 CALIF. L. REV. 513, 539 (2015).

70. *See* Greg Satell, *Three Reasons To Believe the Singularity Is Near*, FORBES (June 3, 2016, 11:19 PM), http://www.forbes.com/sites/gregsatell/2016/06/03/3-reasons-to-believe-the-singularity-is-near [http://perma.cc/5BBK-KN3M].

71. *See, e.g.*, Calo, *supra* note 69, at 541 (describing a Twitter algorithm designed for Stephen Colbert that automatically switches Fox News anchors' names with the titles of movies reviewed by Rotten Tomatoes).

72. *See, e.g.*, FED. R. EVID. 801(d)(2).

cognition," and it is a characteristic of all expert testimony,[73] including that informed by technology.[74] It is why experts are allowed to testify based on hearsay: otherwise, the proponent would be forced to call the Ph.D. advisor, and friends and family of a patient diagnosed with a mental illness in part based on such witnesses' representations, to the stand.[75] In the case of machines, juries might sometimes need the testimony of the machine's "advisor"—the programmer—to adequately assess credibility, particularly since the machine cannot use its own judgment in deciding how much to rely on the instructions or assertions of its programmer.[76] But any ruling allowing the programmer to testify should not be based on the premise that the programmer is the true declarant of the machine's conveyance of information.

The second theoretical objection might be that machine sources are inherently different from human sources because machines do not engage in thought. But that premise, too, is questionable. While Western science has been dominated for centuries by a "passive-mechanistic" view that treats artificial beings as lacking agency, a competing line of thought has insisted that machines have agency, just like living beings, in that their actions are neither random nor predetermined.[77] The father of modern computing, Alan Turing, famously suggested that a machine should be described as "thinking" so long as it could pass as human upon being subject to text-based questioning by a person in another room.[78] "Machine cognition" is now an established field of study,[79] and some have argued for a new "ontological category" for robots, between humans and inanimate objects.[80]

Although it seems clear that machines lack the ability to engage in moral judgment or to "intend" to lie, the need for credibility testing should not turn on whether a source can exercise moral judgment. The coherence of "machine

---

73. *See generally* Jennifer Mnookin & David Kaye, *Confronting Science: Expert Evidence and the Confrontation Clause*, 2012 SUP. CT. REV. 99 (discussing "distributed cognition").

74. *See* Dror & Mnookin, *supra* note 24, at 47.

75. *See, e.g.*, FED. R. EVID. 703 (allowing experts to testify based on hearsay, if of the type reasonably relied upon by experts in the field).

76. *See* discussion *infra* Section III.A.4 (suggesting that meaningful credibility testing of machines might require live testimony of those offering assertive inputs).

77. *See generally* JESSICA RISKIN, THE RESTLESS CLOCK (2016).

78. A. M. Turing, *Computing Machinery and Intelligence*, 59 MIND 433 (1950).

79. *See, e.g.*, Prakash Mondal, *Does Computation Reveal Machine Cognition?*, 7 BIOSEMIOTICS 97, 99-100 (2014).

80. *See* Peter H. Kahn, Jr. et al., *The New Ontological Category Hypothesis in Human-Robot Interaction*, 6TH INT'L CONF. ON HUM.-ROBOT INTERACTION 159 (2011).

credibility" as a legal construct depends on whether the construct promotes decisional accuracy, not on what cyberneticists or metaphysicists have to say about whether a machine can ever achieve "real boy" status. Legal scholars have similarly acknowledged that the question whether machine-generated communications can be "speech" for purposes of the First Amendment is "necessarily a normative project" that rests on one's conception of why certain communications are labeled "speech" at all.[81] If one believes "speech" as a legal category is intended primarily to protect explicitly political expressions, then much algorithm-generated speech might not be covered. If it is intended to promote truth by expanding the marketplace of ideas, then more machine speech might be covered.[82] In the same respect, the question whether to subject machine evidence to credibility testing is a normative project. If one views the law of testimony as intended to promote decisional accuracy, and if black box dangers are not sufficiently guarded against under existing laws treating machine evidence as simply physical objects, then "machine testimony" is a category worthy of study.

B. Black Box Dangers: Causes of Inferential Error from Machine Sources

This Section explores the potential testimonial infirmities of machine sources. Some courts and scholars assume that "machines . . . fall outside the scope of hearsay 'because the hearsay problems of perception, memory, sincerity and ambiguity have either been addressed or eliminated.'"[83] It is true that machine conveyances are not "hearsay," but not because they are immune from testimonial infirmities. While machines might be incapable of "memory loss," a

---

81. Tim Wu, *Machine Speech*, 161 U. PA. L. REV. 1495, 1529 (2013) (arguing that search engine results that merely index information are "tools" rather than speech); *see also* Stuart Minor Benjamin, *Algorithms and Speech*, 161 U. PA. L. REV. 1445 (2013) (arguing, in engagement with Wu, that search engine results are, indeed, speech, because they convey substantive information reflective of the programmer's discretion); Toni M. Massaro & Helen Norton, *Siri-ously? Free Speech Rights and Artificial Intelligence*, 110 NW. U. L. REV. 1169, 1172-73 (2016) (arguing that "computer speakers" might, with further AI developments, be protected under the First Amendment under various conceptions of "speech").

82. *See* Wu, *supra* note 81, at 1507 (discussing different First Amendment theories).

83. Jonathan D. Frieden & Leigh M. Murray, *The Admissibility of Electronic Evidence Under the Federal Rules of Evidence*, 17 RICH. J.L. & TECH. 1, 27 (2011) (quoting PAUL R. RICE, ELECTRONIC EVIDENCE: LAW AND PRACTICE 200 n.12 (2005)); *see also* State v. Armstead, 432 So. 2d 837, 840 (La. 1983) (reasoning that machine testimony is not hearsay because "there is no possibility of a conscious misrepresentation, and the possibility of inaccurate or misleading data only materializes if the machine is not functioning properly").

given machine conveyance—just like a human assertion—might be false or misleading because the machine is programmed to render false information (or programmed in a way that causes it to learn to do so), is inarticulate, or has engaged in analytical missteps.[84]

1. Human and Machine Causes of Falsehood by Design

Merriam-Webster defines "insincere" as "not expressing or showing true feelings."[85] A machine does not have "feelings," nor does it suffer moral depravity in the form of a questionable character for truthfulness. But it could be deliberately programmed to render false information or programmed to achieve a goal in a way that leads the machine itself to learn to utter falsehoods as a means of achieving that goal.

Falsehood by human design. First, humans can design a machine in a way they know, or suspect, will lead a machine to report inaccurate or misleading information. A designer could choose to place inaccurate markings on a mercury thermometer's side, or choose to place alcohol instead of mercury in the bulb during construction, both causing falsity by design. One recent example is the discovery that "[r]ogue [e]ngineers"[86] at Volkswagen used "covert software" to program diesel vehicles to report misleading emissions numbers during pollu-

---

84. One could modify Laurence Tribe's "Testimonial Triangle," his famous schematic for understanding the hearsay dangers, to account for machines. *See* Tribe, *supra* note 59, at 959. The chain of inference would run from "A" (the action or utterance of the machine), to "R" (the result of the machine's process), to "C" (the conclusion to which R points). The left side of the triangle (from "A" to "R") would involve falsehood by design and inarticulateness dangers; the right side (from "R" to "C") would involve analytical errors. One could similarly modify Richard Friedman's classic "route analysis" schematic, which visualizes a "truth path" from a true event, X, to the declarant testifying to X, and details how testimonial infirmities can lead from "not-X" to "testimony(X)." *See* Friedman, *supra* note 15, at 687. If a suspect's BAC is lower than .09% (not-09%), and a machine is programmed correctly and does not compute the BAC as .09%, the machine might nonetheless report .09%, ending up in "testimony(.09%)," if it has been programmed or has taught itself to deceive, has been miscalibrated (inarticulateness), or has received an input of residual mouth alcohol rather than deep lung air (ambiguity or analytical error due to false inputs or misplacement).

85. *See Insincere*, MERRIAM-WEBSTER ONLINE, http://www.merriam-webster.com/dictionary/insincere [http://perma.cc/P657-XT6Q]; *see also Sincere*, OXFORD LIVING DICTIONARIES, http://en.oxforddictionaries.com/definition/sincere [http://perma.cc/MC2D-DVWT] (defining "sincere" as "proceeding from genuine feelings").

86. Chessman, *supra* note 16, at 125 n.80 (citing David Kravets, *VW Says Rogue Engineers, Not Executives, Responsible for Emissions Scandal*, ARSTECHNICA (Oct. 8, 2015), http://arstechnica.com/tech-policy/2015/10/volkswagen-pulls-2016-diesel-lineup-from-us-market [http://perma.cc/YSJ8-DYDQ]).

tion tests.[87] Similarly, two *Time Magazine* journalists were able to determine, through Turing Test-like questioning, that a robot-telemarketer was programmed to falsely claim she was a real person.[88] When one asks Siri, "are you a liar?", her response is "no comment."[89] So long as programming technology exists, and motives to lie or cheat exist, programmers face the "temptation to teach products to lie strategically."[90]

Falsehood by machine-learned design. A machine might also "teach" itself to lie as a strategy for achieving a goal. Once algorithms with "billions of lines of code" and "an enormous number of moving parts are set loose," they go on to "interact with the world, and learn and react," in ways that might be unpredictable to the original programmers.[91] Even if a human does not program a machine to render false or misleading information, the machine can teach itself to lie if it learns that deception is a good strategy to reach a goal programmed into it.[92] In one study, "hungry" robots "learned" to suppress information that clued in other robots to the location of a valuable food source.[93] A legal system should establish safeguards to detect and avoid false or misleading machine testimony, whether the falsity is due to human design or machine-learning.[94]

---

87. Rebecca Wexler, *Convicted by Code*, SLATE (Oct. 6, 2015), http://www.slate.com/blogs/future_tense/2015/10/06/defendants_should_be_able_to_inspect_software_code_used_in_forensics.html [http://perma.cc/TE6T-XR44].

88. Zeke Miller & Denver Nicks, *Meet the Robot Telemarketer Who Denies She's a Robot*, TIME (Dec. 10, 2013), http://newsfeed.time.com/2013/12/10/meet-the-robot-telemarketer-who-denies-shes-a-robot [http://perma.cc/H8S8-2LRE].

89. Test of Apple Siri (Oct. 21, 2016).

90. Marcelo Rinesi, *VW's Fraud Reveals a Troubling Future: Our Machines Can Now Lie*, FAST COMPANY DESIGN (Oct. 1, 2015), http://www.fastcodesign.com/3051753/vws-fraud-reveals-a-troubling-future-our-machines-can-now-lie [http://perma.cc/HN47-YJKJ]. One of the more famous popular culture examples of a computer programmed to lie is HAL 9000. ARTHUR C. CLARKE, 2001: A SPACE ODYSSEY (1968).

91. Tufekci, *supra* note 68.

92. *See, e.g.*, Alan R. Wagner & Ronald C. Arkin, *Acting Deceptively: Providing Robots with the Capacity for Deception*, 3 INT'L J. SOC. ROBOTICS 5, 5 (2011) (noting the ability to "develop an algorithm which allows an artificially intelligent system to determine if deception is warranted in a social situation").

93. Sara Mitri et al., *The Evolution of Information Suppression in Communicating Robots with Conflicting Interests*, 106 PROC. NAT'L ACAD. SCI. 15,786, 15,787-88 (Sept. 15, 2009) (noting that robots "learned" to suppress information that clued in other robots to the location of a food source).

94. *See* discussion *infra* Section III.A.1.

2. *Human and Machine Causes of Inarticulateness*

Like a human source, a machine source might utter information that is inarticulate in a way that leads an observer to draw the wrong inference, even if the machine is otherwise nondeceptive and well designed to render an accurate claim. A machine's reasons for being inarticulate are, like its reasons for being deceptive, different from those of a human witness. A machine does not slur its words due to intoxication or forget the meaning of a word. But a machine can be imprecise, ambiguous, or experience a breakdown in its reporting capacity due to human design, input, and operation errors, as well as machine errors caused by degradation and environment.

Human design. Human design choices—unless disclosed to the factfinder—can lead to inferential error if a machine's conveyance reflects a programmed tolerance for uncertainty that does not match the one assumed by the factfinder. Imagine a human eyewitness tells a police officer at a lineup that he is "damn sure" the man who robbed him is suspect number five. Assume that if the defendant were able to cross-examine the eyewitness in court, the witness would clarify that, to him, "damn sure" means a subjective certitude of about eighty percent. But if the eyewitness never testifies and the prosecution calls the officer to relate the witness's hearsay account, the factfinder might inaccurately infer that "damn sure" means a subjective certitude of ninety-nine percent. Machine conveyances might suffer the same ambiguity. If IBM's Watson were to start conducting autopsies and reporting to factfinders—using a subjective scale—the likely cause of death in criminal cases based on a diagnostic algorithm, factfinders would not know—based solely on Watson's output that the decedent "most likely" suffered from a particular condition—whether their own tolerance for uncertainty matched Watson's. DNA match statistics generated by software, offered without information about the size of potential sampling error in the population frequency estimates used, would be another example,[95] as would medical diagnosis algorithms, where software designers must make decisions about how far to tolerate false negatives and positives.[96] This sort of failure to articulate a tolerance for uncertainty produces *ambiguity*. In contrast, a machine that is over- or underconfident in its assessment—that

95. *See, e.g.*, James M. Curran, *An Introduction to Bayesian Credible Intervals for Sampling Error in DNA Profiles*, 4 LAW PROBABILITY & RISK 115, 115-16 (2005) (noting the inevitability of sampling error in DNA match statistics and suggesting that sampling error estimates be presented in court).

96. *See* Felicitas Kraemer et al., *Is There an Ethics of Algorithms?*, 13 ETHICS & INFO. TECH. 251, 251 (2011).

is, one that states a level of uncertainty about its assessment that does not correspond to the actual empirical probability of the event—suffers another sort of infirmity,[97] whether an analytical error or falsehood by design.

Human operation. A human operator could also create ambiguity leading to inferential error by placing the machine in circumstances where its conveyance of information is misleading. Again analogizing to human testimony, imagine 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.[98] 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.[99]

Machine degradation and malfunction. Due to entropy, machines stray from their original designs over time and potentially err in articulating their calculations. A digital thermometer's battery might wear out to the point that "eights" appear to be "sixes." A bathroom scale might be bumped such that—absent consistent calibration—it no longer starts its measurements at zero, thus overreporting weight. One could conceive of these errors as "machine errors," because the machine has lost its ability to articulate, or as human maintenance errors, because an operator failed to take corrective action. The critical point is that, when left unattended, machines can malfunction in ways that manifest as inarticulate conveyances.

3. Human and Machine Causes of Analytical Error

In the early days of computing, some philosophers rejected the idea that a machine could "perceive" anything.[100] Now, numerous universities have laboratories dedicated to the study of "machine perception,"[101] from the devel-

---

97. *See* MacCoun, *supra* note 33, at 200.

98. *Cf.* Paul Bergman, *Ambiguity: The Hidden Hearsay Danger Almost Nobody Talks About*, 75 KY. L.J. 841, 861-62 (1986) (describing the "natural tendency to amplify stories by adding details and meanings to them" as a form of "ambiguity").

99. *See* Sosa, *supra* note 15, at 117 ("If the thermometer is to tell the ambient temperature reliably, it must be appropriately situated in certain contingent ways . . . .").

100. *See, e.g.*, Alan Gauld, *Could a Machine Perceive?*, 17 BRIT. J. FOR PHIL. SCI. 44, 46 (1966).

101. *See, e.g.*, Bradley Dep't of Elec. & Comput. Eng'g, *Research Areas: Machine Perception*, VIRGINIATECH, http://www.ece.vt.edu/research/area/perception [http://perma.cc/Y8FP-X3ZR].

opment of hardware allowing machines to approximate human senses such as touch, vision, and hearing, to aesthetic judgment about art.[102] Some machines are much cruder, "perceiving" only in the sense of interacting with and analyzing data. Given these ongoing debates about the differences between machine and human perception, I use the term "analytical error" rather than "misperception" to capture machine errors analogous to human cognitive and perceptive errors.

Human design. Analytical errors can stem from programming mistakes, beginning with inadvertent miscodes. Miscodes are inevitable; "bugs and misconfigurations are inherent in software."[103] In several cases, programmers have failed to program computer codes that could accurately translate legal code.[104] Likewise, programmers have miscoded crime-detecting and forensic identification tools, which has led to inaccurate analysis of allelic frequencies, embedded in DNA-typing software to generate match statistics;[105] to glitches in Apple's "Find My iPhone" App that have led victims of iPhone theft and loss to the wrong locations;[106] and to a "minor miscode" in a probabilistic DNA-genotyping software program that affected the reported match statistics in several cases, though generally not by more than an order of magnitude.[107] Other notorious miscode examples include the Therac-25, a computer-controlled ra-

102. *See, e.g.*, Emily L. Spratt & Ahmed Elgammal, *Computational Beauty: Aesthetic Judgment at the Intersection of Art and Science*, *in* 1 COMPUTER VISION: ECCV 2014 WORKSHOPS 35, 41 (Lourdes Agapito et al. eds., 2014).

103. Sergey Bratus et al., *Software on the Witness Stand: What Should It Take for Us To Trust It?*, *in* TRUST AND TRUSTWORTHY COMPUTING 396, 397 (Alessandro Acquisti et al. eds., 2010).

104. *See, e.g.*, Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1268-71 (2008) (noting that the automated public benefits systems of Colorado, California, and Texas mistranslated codified eligibility requirements and erroneously distributed or withheld public benfits); Steven R. Lindemann, *Published Resources on Federal Sentencing*, 3 FED. SENT'G REP. 45, 45-46 (1990) (noting a potential for errors in the federal sentencing guidelines' software, ASSYST).

105. *See Notice of Amendment of the FBI's STR Population Data Published in 1999 and 2001*, FED. BUREAU INVESTIGATION (2015), http://www.fbi.gov/about-us/lab/biometric-analysis/codis/amended-fbi-str-final-6-16-15.pdf [http://perma.cc/FR35-44TN].

106. *See* Lawrence Mower, *If You Lose Your Cellphone, Don't Blame Wayne Dobson*, LAS VEGAS REV.-J. (Jan. 13, 2013), http://www.reviewjournal.com/news/las-vegas/if-you-lose-your-cellphone-dont-blame-wayne-dobson [http://perma.cc/WRN6-3Z4D].

107. *See* David Murray, *Queensland Authorities Confirm 'Miscode' Affects DNA Evidence in Criminal Cases*, 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 [http://perma.cc/Z8HP-Y2H3].

diation therapy machine that "massively overdosed" six people in the late 1980s based on a software design error.[108]

Human design could also lead a machine to utter false or misleading information where the programmer makes inappropriate analytical assumptions or omissions. Programmers must incorporate a number of variables to ensure that machine estimates are accurate. For example, programmers must design breath-alcohol machines to distinguish between ethyl alcohol, the alcohol we drink, and other substances, such as acetone, that present similar profiles to a machine relying on infrared technology.[109] They must also program breath-alcohol machines with an accurate "partition ratio" to calculate blood-alcohol level from the suspect's breath-alcohol level, a ratio that some defense experts say differs nontrivially from person to person.[110] An expert review of the "Alcotest 7110" source code found that, although the device was "generally scientifically reliable," its software had several "mechanical and technical shortcomings."[111] This review prompted the New Jersey Supreme Court to require modifications to the machine's programming to guard against misleadingly high readings.[112] Moreover, in modeling highly complex processes, a programmer's attempt to account for one variable might inadvertently cause another variable to lead to error. For example, Tesla now believes that the fatal crash of one of its self-driving cars into a truck trailer might have occurred because the car's radar detected the trailer but discounted it as part of a design to "tune out" certain structures to avoid "false braking."[113]

A programmer's conscious or unconscious bias might also influence algorithms' predictions or statistical estimates. For example, software designers have created compliance and risk-management software with "automation bi-

---

108. Nancy G. Leveson, *Medical Devices: The Therac-25 Story*, *in* SAFEWARE: SYSTEM SAFETY AND COMPUTERS app. A (1995).

109. *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., DOT-HS-806-922, THE LIKELIHOOD OF ACETONE INTERFERENCE IN BREATH ALCOHOL MEASUREMENT (1985).

110. *See, e.g.*, People v. Vangelder, 312 P.3d 1045, 1057–58 (Cal. 2013); *see also id.* at 1061 (explaining the "partition ratio," but noting that a California statute "rendered irrelevant and inadmissible defense expert testimony regarding partition ratio variability among different individuals").

111. New Jersey v. Chun, 943 A.2d 114, 120-21 (N.J. 2008).

112. *Id.* at 172-74.

113. David Shepardson, *Tesla Mulling Two Theories To Explain 'Autopilot' Crash: Source*, REUTERS (July 29, 2016), http://www.reuters.com/article/us-tesla-autopilot-congress-idUSKCN10928F [http://perma.cc/2JM9-B6BM].

ases" to favor corporate self-interest,[114] and Facebook recently rigged its "trending topics" algorithms to favor ideologically liberal content, a result the company insists was caused by "unconscious bias" on the part of human curators.[115] And algorithm-generated credit scores and dangerousness "scores" may entrench bias by incorporating racially-correlated variables.[116] In addition to designer bias, user patterns can inadvertently skew algorithms. For example, the *WestlawNext* algorithm may have the "potential to change the law" by biasing results away from "less popular legal precedents" and rendering those precedents "effectively . . . invisible."[117]

Even if a programmer is not "biased" in the sense of making choices to further a preconceived goal, her analytically controversial choices can affect the accuracy of the machine's scores and estimates. For example, in the DNA context, programmers have the power to set thresholds for what to count as a true genetic marker versus noise in determining which markers to report on the graphs used in determining a match.[118] Programmers of DNA mixture interpretation software must also decide how conservative their estimates should be with respect to the probability of unusual events—such as small amounts of contamination during testing—that directly affect interpretation.[119] Beyond the interpretation of the DNA sample itself, programmers must make judgment

---

114. *See* Kenneth A. Bamberger, *Technologies of Compliance: Risk and Regulation in a Digital Age*, 88 TEX. L. REV. 669, 676 (2010).

115. Mike Isaac, *Facebook 'Trending' List Skewed by Individual Judgment, Not Institutional Bias*, N.Y. TIMES (May 20, 2016), http://www.nytimes.com/2016/05/21/technology/facebook-trending-list-skewed-by-individual-judgment-not-institutional-bias.html [http://perma.cc/MR5X-B7WH].

116. *See, e.g.*, Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 10-16 (2014); Sonja B. Starr, *Evidence-Based Sentencing and the Scientific Rationalization of Discrimination*, 66 STAN. L. REV. 803, 838 (2014).

117. Ronald E. Wheeler, *Does* WestlawNext *Really Change Everything? The Implications of* WestlawNext *on Legal Research*, 103 LAW LIBR. J. 359, 368 (2011).

118. *See* JOHN BUTLER, ADVANCED TOPICS IN DNA TYPING: INTERPRETATION 40-44 (2014); *see also* Roberts v. United States, 916 A.2d 922, 933-34 (D.C. Cir. 2007) (discussing the FBI's default interpretation settings, and noting that a "stutter" threshold was dispositive in Roberts's case as to inclusion or exclusion).

119. In DNA mixtures involving small quantities of DNA, some alleles might "drop out" of the resulting graphs even when they were actually present in the evidence source, while others "drop in" to the graphs due to small amounts of contamination. DNA mixture software must incorporate estimates for the rates of drop-in and drop-out, both in generating match statistics and in concluding whether a suspect is a potential contributor to a mixture. BUTLER, *supra* note 118, at 165, 170-73; *see also* ERIN E. MURPHY, INSIDE THE CELL: THE DARK SIDE OF FORENSIC DNA 74-82 (2015).

calls that affect the software's report of a match statistic, such as determining the appropriate reference population for generating estimates of the rarity of genetic markers.[120]

Machine-learning in the design stage. Machines themselves might also augment their programming in ways that cause analytical errors. Machines learn how to categorize new data by training on an existing set of data that is either already categorized by a person ("supervised learning") or is categorized by the computer itself using statistics ("unsupervised learning").[121] The fewer the samples in the training set,[122] or the more that future data is likely to look different from the training set over time,[123] the greater the chance the algorithm will draw an incorrect inference in future observations. Errors might occur because the machine infers a pattern or linkage in the limited data set that does not actually mirror real life ("overfitting").[124] Or the machine might try to account for too many variables, making the data set inadequate for learning (the "curse of dimensionality"),[125] a reason that match-dating websites catering to narrower subgroups predict matches better.

In the crime-detecting context, imagine a machine like the Avista SmartSensor[126] that teaches itself, after seeing how police categorized three hundred street level interactions through surveillance camera footage, that a person who shakes hands three times in a row is likely engaged in a drug trans-

---

120. As part of calculating its match-statistic, the software must calculate the frequency of various genotypes in some relevant population. Laboratories in the United States typically calculate DNA match-statistics based on the FBI's allelic frequency tables, which are in turn based on samples from particular populations. BUTLER, *supra* note 118, at 214, 245-47. The choice of population matters: if a court in Northern Ireland wanted to have an accurate sense of the chance that a black defendant's DNA profile was consistent with a mixture purely by chance, where the defendant was a long-time local resident, the court might use the United Kingdom's Afro-Caribbean database rather than the FBI's African-American database. *Id.* at 250.

121. ROBERT J. GLUSHKO ET AL., THE DISCIPLINE OF ORGANIZING: INFORMATICS EDITION 336 (Robert J. Glushko ed., 4th ed. 2016).

122. *See* Surden, *supra* note 19, at 92 (noting that a machine learning algorithm "may perform poorly at first when it has only had a few examples of a phenomenon . . . from which to detect relevant patterns").

123. Imagine, for example, a machine algorithm that recommends new articles, where the trending topics change daily. Data science scholars call this problem "distribution drift." ALICE ZHENG, EVALUATING MACHINE LEARNING MODELS: A BEGINNER'S GUIDE TO KEY CONCEPTS AND PITFALLS 3 (2015).

124. PEDRO DOMINGOS, THE MASTER ALGORITHM: HOW THE QUEST FOR THE ULTIMATE LEARNING MACHINE WILL REMAKE OUR WORLD 71 (2015).

125. *See, e.g.*, *id.* at 186-90.

126. *See* Rich, *supra* note 67, at 873 n.3.

action. Even if this new decision rule were reasonable based on the machine's sample, an inference in a future case that two people are engaged in illegal activity based on that new programming might be incorrect. Alternatively, a machine might inaccurately infer that a crime is *not* occurring.

Human input and operation. Some machines do not require further human input, post-design, before conveying information. A mercury thermometer, for example, does not require a person to input information or physical objects before reporting ambient temperature. Even a highly complex "lay" machine, such as a robot security guard reporting what it has seen, is able to convey information based solely on its programming and the events it perceives. On the other hand, many machines do require human input to convey information. These human inputs can be either "physical" or "assertive," but both types of input can lead to erroneous machine conveyances.

Assertive input encompasses information that humans enter into machines. Most "expert systems"—programs rendering complex analysis based on information fed to it by humans—require inputters to provide case-specific information, and those types of machines might misanalyze events or conditions if fed the wrong inputs. For example, DNA mixture interpretation software might require a human analyst to upload the DNA profile information of a typed sample before conducting its analysis. Similarly, a medical diagnosis expert system might require a human doctor to upload patient information.[127]

The potential for error stemming from expert systems' reliance on the assertions of human inputters is analogous to the potential for error from human experts' reliance on the assertions of others. The law of evidence generally shields juries from human testimony that merely repeats the assertions of others. Thus, as a general rule, lay witnesses are forbidden from testifying to statements made by others, on grounds that the hidden declarant's testimonial capacities cannot be tested.[128] But human experts may base their opinions in part on otherwise-inadmissible assertions made by other people, so long as those assertions are of the type "reasonably relied upon" by experts in the

127. Machine operators might also have to input case-specific analysis parameters. *See, e.g.*, Letter from Mark W. Perlin, Chief Sci. & Exec. Officer, Cybergenetics, to Jerry D. Varnell, Contract Specialist, Fed. Bureau of Investigation 3 (Apr. 1, 2015) [hereinafter Perlin Letter] (noting that some programs "give different answers based on how an analyst sets their input parameters"). Conceptually, errors in case-specific parameters seem more naturally labeled as programming errors causing misperception than as false input errors.

128. *See, e.g.*, FED. R. EVID. 601, 801(d); Morgan, *supra* note 17, at 178-79 (discussing the rules surrounding hearsay testimony).

field.[129] A human psychologist's assertion that the defendant suffers from schizophrenia is likely a product of her schooling, the treatises and articles she has read, and the interviews she conducted with the defendant's friends and family. In short, her assertion is a product of what evidence scholars have called "distributed cognition."[130] While distributed cognition is an inevitability of expert testimony, the possibility that these other assertions are false necessarily injects another potential source of error into an expert's, or expert system's, analysis.

Other problematic inputs leading to a false machine conveyance might be physical rather than assertive. 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.[131] 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.[132] "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.[133]

Machine error. Finally, analytical error can stem from machine malfunction due to degradation or environmental factors. A digital thermometer left rusting in the rain might experience a glitch in its computational process and render an incorrect result. A voltage change might cause a breath-testing machine's process to malfunction during its analysis, leading to inaccurate results.[134] An ini-

---

129. FED. R. EVID. 703.

130. *See* Dror & Mnookin, *supra* note 24, at 1-4.

131. *See* JEANNE SWARTZ, AM. PROSECUTORS RESEARCH INST., BREATH TESTING FOR PROSECUTORS: TARGETING HARDCORE IMPAIRED DRIVERS 12, 14-15 (2004).

132. *See, e.g.*, Andrea Roth, *Defying DNA: Rethinking the Role of the Jury in an Age of Scientific Proof of Innocence*, 93 B.U. L. REV. 1643, 1676-79 (2013) (cataloging instances of DNA false positives due to contamination, as well as instances in which the prosecution has claimed that contamination explains a DNA exclusion).

133. *See, e.g.*, Florence v. Bd. of Chosen Freeholders, 132 S. Ct. 1510 (2012) (holding that a strip search based on a warrant erroneously still in the computer system was legal); Herring v. United States, 555 U.S. 135 (2009) (holding that items obtained in an arrest on a warrant still erroneously in the computer system were not excludable under the Fourth Amendment); Arizona v. Evans, 514 U.S. 1 (1995) (same).

134. *See, e.g.*, *In re* Source Code Evidentiary Hearings in Implied Consent Matters, 816 N.W.2d 525, 531 (Minn. 2012) (noting one expert's testimony that a breath-testing machine could

tially functioning computer program might experience "software rot," a deteriorating and outdating of code over time that, if not subject to periodic software review that could detect such deterioration, could cause a machine to render false or misleading information. Or even an errant animal might be to blame.[135] In 2009, according to an Air Force spokesman, a control room temporarily lost contact with Reaper and Predator drones at an American Air Force command base after a cat wandered in and "fried everything."[136]

***

The fact that machine evidence might implicate black box dangers does not necessarily mean it should be excluded or even subject to special safeguards. It may be that for a particular type of conveyance, the likelihood that black box dangers would both exist and be discounted by the jury is low, and that the cost of exclusion or production of further contextual information is too high. The goal of this Article is not to allow opponents of machine evidence to capitalize on the cachet of labels like "credibility" in arguing for broad exclusion of potentially risky machine conveyances.[137] Rather, it is to force lawmakers, scholars, courts, and litigants to recognize that some machine sources will likely benefit from at least some of the credibility-testing mechanisms we use in the human context, for some of the same reasons that human sources benefit from such testing.

II. A TAXONOMY OF MACHINE EVIDENCE

Armed with the black box dangers framework, this Part explores which machine acts and utterances implicate credibility, and how courts have attempted to regulate them. As it turns out, courts, scholars, and litigants have

render inaccurate readings in the event of a "power drift," and that the source code revealed no means of detecting or reporting such a voltage change).

135. *See* Chessman, *supra* note 16, at 121 (citing Clemente Izurieta & James M. Bieman, *A Multiple Case Study of Design Pattern Decay, Grime, and Rot in Evolving Software Systems*, 21 SOFTWARE QUALITY J. 289, 290 (2013)).

136. Lewis Page, *'Al Qaeda Suicide Cat' Sends US Iraq War Robots out of Control*, REGISTER (Apr. 19, 2010, 2:44 PM), http://www.theregister.co.uk/2010/04/19/us_war_robots_out_of_control_cat_strike [http://perma.cc/NC8S-Y6J7] (quoting an unidentified officer).

137. Indeed, some have argued that the term "reliability" should be used for human witnesses, with the term "credibility" reserved for "evidence." *See* Schum, *supra* note 15, at 23 (citing MARCUS STONE, CROSS-EXAMINATION IN CRIMINAL TRIALS 41-44 (1988)).

often implicitly recognized that some machines do what witnesses do: they make claims relied upon by factfinders for their truth. But these intuitions have not translated into a systematic regime of machine credibility testing.

A. Machine Evidence Not Dependent on Credibility

Some human acts and utterances do not implicate the credibility of the actor or speaker. Evidence that a defendant was having an affair might be offered as circumstantial proof of a motive to kill his wife. A party may offer evidence that a person said "it's cold out here" after an accident merely to prove the person was conscious and able to speak at the time of the statement, and not to prove that the temperature was actually low. These acts and utterances do not implicate the sincerity, articulateness, memory, or perception of the human actor. Instead, they are essentially akin to physical objects, whose mere existence the proponent invokes in persuading the factfinder to draw a particular inference.

Like human acts and utterances, machine testimony does not always raise concerns about the credibility of the machine source itself. Machine evidence does not implicate the black box dangers—the testimonial infirmities of machine sources—when the machine acts simply as a conduit for the assertions of others; when it simply performs an act that facilitates scientific testing; or when its conveyance is offered for a purpose other than its truth.

Critically, it is not the complexity or type of machine that determines whether machine evidence implicates credibility. The most opaque, complex, biased, manipulable machine imaginable might produce evidence that is not dependent on credibility, for example, if the evidence is a printout offered simply to show that the machine's ink cartridge was functioning at the time. Likewise, proprietary email software that simply offers a platform for the emailed assertions of human communicators, themselves offered for their truth, does not implicate black box dangers simply because it is proprietary. These types of machine evidence might affect decisional accuracy by implicating *authenticity* concerns, requiring proof that the machine result is what the proponent says it is—an email actually written by Aunt Mary, or a printout from a particular machine. But they do not implicate *black box* concerns.

1. Machines as Conduits for the Assertions of Others

Some machines act as "conduits" for the assertions of people, and thus do not implicate the black box dangers.[138] For example, if I write my friend an email stating that "John ran the red light," and a party introduces my email in a civil suit as proof that John ran the red light, the assertion is mine, not the machine's. The same logic would apply to tape recorders and dictographs, text messages, website or social media content, and any "electronically stored information" (ESI),[139] such as databases listing entries made by employees.[140]

The line between a machine conduit and a machine source implicating black box dangers is not necessarily a bright one.[141] For example, automatic transcription services such as Google Voice can be "extremely inaccurate" under certain conditions, such as when a speaker has a heavy accent.[142] Google Voice might therefore raise the specter of analytical error, and thus might require credibility testing, in a way that a tape recorder does not. The ability of email, internet content, or a tape recording to be manipulated, however, does not render the resulting product the conveyance of a machine source rather than a conduit. Rather, the doctored information would be akin to a doctored transcript or fabricated physical object. The admission of such evidence may turn on authenticating whether the human declarant actually made the statement, but it raises no novel issue of machine credibility.[143] And, usually, a proponent

---

138. A court reporter or translator regurgitating the statements of another person is often treated as a human conduit for that other person's statements, rather than as a witness herself. *See generally* 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 (discussing the hearsay and Confrontation Clause problems raised by the introduction of a transcript of the witness's testimony into evidence).

139. ESI has been explicitly incorporated into civil discovery rules. *See* FED. R. CIV. P. 34.

140. *See, e.g.*, United States v. Liebert, 519 F.2d 542, 543 (3d Cir. 1975) (discussing a list of persons not filing tax returns that was stored on IRS computers).

141. *Cf.* Nicolas, *supra* note 138, at 1159-60 & nn.46-48 (noting nontrivial issues of human conduit accuracy, where courts will treat the conduit as a hearsay declarant).

142. *See* George Cornell, Note, *The Evidentiary Value of Automatically Transcribed Voicemail Messages*, 17 B.U. J. SCI. & TECH. L. 259, 283 & n.185 (2011) (discussing evidentiary issues raised by the inaccuracy of Google Voice and other automatic transcription services).

143. *See, e.g.*, Jerold S. Solovy & Robert L. Byman, *Don't Let Your E-Evidence Get Trashed*, NAT'L L.J. (June 12, 2007), http://www.nationallawjournal.com/id=900005483411/Dont-Let-Your-EEvidence-Get-Trashed [http://perma.cc/A4QV-E67P] (noting that "altering an e-mail takes nothing more than an impure heart and a keystroke" and that "to be admissible, [a litigant] will need to show, among other things, that [an e-mail] is authentic and it is not hearsay").

of ESI is required to authenticate the information by showing the input and recording process was regular.[144] Authentication ensures that the computer faithfully rendered another person's assertion. The person's assertion itself, of course, is subject to all the usual safeguards that apply to human testimony.

2. Machines as Tools

Machine evidence also does not implicate black box dangers when offered to show that human witnesses used the machines as tools to facilitate their observations. Examples might include a laser that facilitates latent fingerprint collection or bloodstain pattern recognition; a magnifying glass or reading light that facilitates handwriting analysis; a gas chromatograph that facilitates the separation of a substance that can then be analyzed by a human or mass spectrometer; and a machine that takes a small amount of DNA and, through repeated heating and cooling cycles, makes millions of copies of the DNA to facilitate later testing.[145] Machine tools are analogous to human laboratory technicians who maintain and operate equipment, or who otherwise offer assistance during testing. Of course, human technicians might deliberately tamper with results in a way that machines would not, unless programmed to do so. But the technicians' actions, while consequential, are not treated as credibility-dependent assertions under hearsay law.

Like the actions of human technicians who facilitate testing, the actions of machine tools are different from machine and human sources that convey information. Instead, the actions of machine tools are akin to physical objects or natural processes.[146] A gun or tape recording cannot be "impeached" because

---

144. *See* Am. Express Travel Related Servs. Co. v. Vinhnee (*In re* Vinhnee), 336 B.R. 437, 446 (B.A.P. 9th Cir. 2005) (adopting an eleven-step test for verifying the authenticity of electronic records).

145. *See, e.g.*, *C1000 Touch™ Thermal Cycler*, BIO-RAD (2016), http://www.bio-rad.com/en-us/product/thermal-cyclers-for-pcr/c1000-touch-thermal-cycler [http://perma.cc/27DS-WBYV] (describing an amplification machine used to create DNA copies offered by the company Bio-Rad Laboratories, Inc.).

146. To be sure, some observers have referred even to natural processes or physical objects as "silent witnesses" offering "testimony." *See, e.g.*, DAMAŠKA, *supra* note 8, at 129 (noting descriptions of natural phenomena as "witnesses"); 1 JAMES BRADLEY THAYER, A PRELIMINARY TREATISE ON EVIDENCE AT THE COMMON LAW: DEVELOPMENT OF TRIAL BY JURY 35 n.1 (1896) (referring to mechanisms in pre-Christian trials by ordeal as "witness[es]"). Such descriptions may have reflected a theoretical confusion among scientists in certain eras about whether "facts" are physical "things" to be discovered and observed, or "words" to be heard or read or spoken. *See* BARBARA J. SHAPIRO, A CULTURE OF FACT: ENGLAND, 1550-1720, at 129

they make no claims; they are authenticated, and then offered to the jury for what they are worth. The same is true for evidence of a machine action offered simply to prove the machine committed a certain act, such as mixing two substances together. The act is relevant for whatever inferences can be directly drawn from it. Similarly, where a machine tool merely illuminates facts for a human observer, the observation and report relied upon by the factfinder is ultimately that of the human witness, not of the machine.[147] A human expert might make a mistake, of course: "[m]icroscopic studies" require "'a sincere Hand, and a faithful eye' to examine and record 'the things themselves as they appear.'"[148] Those who criticize microscopic hair analysis as a means of forensic identification do so on the grounds that examiners suffer cognitive bias and lack any probabilistic basis for determining the probative value of an alleged match,[149] not on grounds that the microscope itself has made an underscrutinized claim.

In contrast, the opinion of a human expert—or an expert system—can be impeached, and the opponent should have the chance to do so.[150] There are difficult cases at the margins, where the difference between a machine tool facilitating human observation and a machine source engaging in its own observation is subtle. A thermal imaging device, for example, while in one sense an object facilitating human observation, is also an observer and interpreter itself,

(2000). In any event, such descriptions are not inconsistent with the thesis that machine conveyances of information implicate black box dangers deserving of scrutiny much like hearsay dangers are deserving of scrutiny.

147. One could imagine a human laboratory worker's acts or utterances being offered as "implied assertions," consistent with a worker's belief that a certain condition is true, and offered to prove the condition is true. The acts or utterances of machine tools might implicate black box dangers if offered for a similar purpose.

148. SHAPIRO, *supra* note 146, at 119 (quoting English inventor Robert Hooke).

149. *See, e.g.*, President's Council of Advisors on Sci. & Tech., *Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods*, EXECUTIVE OFF. PRESIDENT 119-21 (2016) [hereinafter PCAST Report], http://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf [http://perma.cc/34K2-98AQ].

150. The Advisory Notes to the American Law Institute's Model Code of Evidence and the Federal Rules of Evidence are both silent on the issue of machine declarants. *See* MODEL CODE OF EVIDENCE ch. VI (AM. LAW INST. 1942); FED. R. EVID. 801 advisory committee's note to proposed rules. The fact that modern codes explicitly exempt nonpersons from the definitions of hearsay appears to have more to do with a fear that bloodhound evidence would be inadmissible if dogs were considered declarants. *See, e.g.*, 2 BYRON K. ELLIOTT & WILLIAM F. ELLIOTT, A TREATISE ON THE LAW OF EVIDENCE § 1253, at 503 (1904) ("It is really the dog that is the witness, and the evidence would seem to be hearsay in this view . . . .").

within the confines of its design and inputs. The device's own credibility—whether its conveyance might be false by design, inarticulate, or analytically unsound—is implicated.

3. *Machine Conveyances Offered for a Purpose Other than Proving the Truth of the Matter Conveyed*

A machine's act or utterance, even if explicitly conveying a claim, does not implicate black box dangers if it is not offered to prove the truth of the claim. In the human context, an act or utterance not offered for its truth does not implicate the so-called "hearsay dangers" (and thus, even if made out of court, does not implicate the hearsay rule) because the inference to be drawn by the factfinder does not "involv[e] a 'trip' into the head of the person responsible . . . ."[151] In the same respect, when a jury can draw the requested inference from a machine act or utterance with no trip into and out of the machine's analytical process, the machine's believability is not at stake.

For example, if a machine's printout were offered merely to prove that the machine's ink toner was functional at the time of printing, then the evidence would not pose a black box problem. The printout is nothing more than a physical object, which the factfinder observes and from whose mere existence the factfinder can draw the proponent's requested inference. Similar logic would apply to statements sent by FBI malware to computers suspected of having visited certain illegal websites, offered not for their truth but to show that the computers then sent information back to the FBI.[152] Likewise with evidence in a fraud case that a red light camera programmer has chosen an unreasonably short "grace period" to generate revenue for the city.[153] The probative value of the statement stems not from its "communicable content," but from its "perceptual content."[154]

---

151. Tribe, *supra* note 59, at 958.

152. *See* Declaration of Matthew Miller at 5, United States v. Michaud, No. 3:15-CR15-5351RJB (W.D. Wash. May 9, 2016), http://www.documentcloud.org/documents/2828710-Michaud-tues2.html#document/p5/a2 [http://perma.cc/N342-MYTE].

153. Daniel Rubin, *In the Dark over Traffic Cameras*, PHILA. INQUIRER, Oct. 9, 2008, at B1.

154. Lackey, *supra* note 48, at 3; *see also* United States v. Khorozian, 333 F.3d 498, 506 (3d Cir. 2003) (holding that the contents of a fax containing the name "Teixiera" were not hearsay because they were offered simply to show that the defendant, accused of bank fraud, was familiar with someone named Teixiera at the time of the transmission).

B. Machine Evidence Dependent on Credibility

This Section explores how courts, scholars, and litigants have historically treated machine evidence that does implicate credibility; that is, machines whose acts and utterances are offered for the truth of some claim they convey in a way that implicates the black box dangers. Even as these groups appear to recognize the "testimony"-like nature of certain machine evidence, these episodes of recognition have never converged to form a single coherent doctrine of machine testimony. Instead, lawmakers have dealt with machine sources through a patchwork of ill-fitting hearsay exceptions, confusing authenticity rules, and promising but inadequate reliability requirements for expert methodologies.

As this Section also explains, machine sources that implicate credibility vary in their characteristics: some are simple, some are complex; some are transparent, some are opaque; some are highly stable, while others are highly sensitive to degradation or human input and operation errors; and some are created in anticipation of litigation, while others have a nonlitigative public or commercial use. Some machine sources convey images, while others explicitly convey information through symbolic output. These characteristics may determine whether a machine source should be subject to particular safeguards, but even the simplest, most transparent, most stable, and most regularly made instrument is a "source" if its output depends on credibility for its probative value.

1. "Silent Witnesses" Conveying Images

When offered as proof of an event or condition they purport to have captured, photographs and films implicate the testimonial capacities of the camera itself, as influenced, of course, by human choices. Jennifer Mnookin, in her exploration of the socio-legal history of the photograph, notes the many courts and commentators who referred to the photograph in its early days in testimonial terms: a "sworn witness,"[155] a "dumb witness,"[156] a "mirror with a memory," in the words of Oliver Wendell Holmes,[157] and even—to the skep-

155. Jennifer L. Mnookin, *The Image of Truth: Photographic Evidence and the Power of Analogy*, 10 YALE J. L. & HUMAN. 1, 17 (1998) (quoting Lady Elizabeth Eastlake, *Photography*, 101 QUARTERLY REV. 465 (1857), *reprinted in* CLASSIC ESSAYS ON PHOTOGRAPHY 39, 65 (Alan Trachtenberg ed., 1980)).

156. *Id.* at 18 (quoting Franklin v. State, 69 Ga. 37, 43 (1882)).

157. *Id.* at 16 (quoting Oliver Wendell Holmes, *The Stereoscope and the Stereograph*, 3 ATLANTIC MONTHLY 738 (1861), *reprinted in* CLASSIC ESSAYS ON PHOTOGRAPHY, *supra* note 155, at 74).

tics—a "most dangerous perjurer,"[158] a witness that, because it cannot be cross-examined, "may testify falsely with impunity."[159] Again, these descriptions were not simply metaphor. They reflected a qualitative difference between photographs and mere physical evidence:

> [P]hotographs, unlike murder weapons, . . . tell a story about the world, making a difficult-to-refute claim about how a particular location looked at one instant . . . . [T]o whatever extent this visual depiction is *not* tied to testimony, a competing, nonverbal account enters a space where the words of witnesses—and lawyers—are supposed to reign.[160]

John Henry Wigmore similarly described the x-ray machine as a conveyor of information, one that "may give correct knowledge, though the user may neither have seen the object with his own eyes nor have made the calculations and adjustments on which the machine's trustworthiness depends."[161] Tal Golan describes the x-ray and other visual evidence as the emblem of a new class of "machine-made testimonies" of the late nineteenth century.[162] Others have more explicitly argued that filmic evidence is inherently "testimonial"[163] and "assertive in nature,"[164] and have, in passing, analogized film to hearsay in arguing that its assertions potentially exhibit insincerity, misperception, and ambiguity.[165]

The camera is a relatively simple machine, in terms of its physical form and internal processes. But because photography is highly sensitive to human input and human bias, photographic evidence can easily mislead a factfinder. A cam-

---

158. *Id.* at 26 (quoting *The Photograph as a False Witness*, 10 VA. L.J. 644, 645-46 (1886), *reprinted in* IRISH L. TIMES & CENTRAL L.J.).

159. *Id.* at 55-56 (quoting Defendant's Brief, Trial Records, Gilbert v. West End Highway (Supreme Judicial Court Records, Social Law Library, Boston, Mass., 1893)).

160. *Id.* at 56.

161. 1 WIGMORE, *supra* note 50, § 665, at 1072.

162. TAL GOLAN, LAWS OF MEN AND LAWS OF NATURE 183-84 (2004).

163. Silbey, *supra* note 15, at 508 n.62.

164. Jessica Silbey, *Cross-Examining Film*, 8 U. MD. L.J. RACE RELIGION GENDER & CLASS 17, 19 (2008); *see also* Caren Myers Morrison, *Body* Camera Obscura*: The Semiotics of Police Video*, 2, 5 (Ga. State Univ. Coll. of Law, Working Paper No. 2016-17), http://ssrn.com/abstract=2826747 [http://perma.cc/HBH4-BVA6] (arguing that police videos "bear[] witness" and further particular narratives rather than an "objective truth").

165. Silbey, *supra* note 164, at 26 n.58.

eraperson might intentionally or through unconscious bias[166] choose a lens, filter, or angle to make a suspect look more sinister[167] or guilty,[168] make a wound seem deeper or shallower,[169] or make a distance seem greater or smaller.[170] Moreover, photographs and film do not provide factfinders with full context. Key aspects of an event or condition might be missed or obscured because of poor sound or visual quality of an image or film,[171] potentially leading a factfinder to draw improper inferences. For day-in-the-life videos and other filmic evidence created expressly for litigation, the motivation for biased representation of facts—such as increasing a film speed to make a disabled subject look less injured[172]—might be particularly high. Photographs can also be modified or fabricated, just like any other physical object. After capturing an image, a photographer may choose to "reverse the negative" so that the right side of the photograph appears on the left side.[173] But these possibilities of post-hoc human manipulation pose problems for authenticity, not credibility.

Courts' treatment of photographic evidence reflects both a promising intuition that black box dangers exist and an unfortunate failure of imagination in fully regulating photographs as credibility-dependent evidence. In photography's early days, courts admitted photographs only if the photographer testified about the process and certified the image's accuracy.[174] This rule addressed a fear that the public would view photographic images as infallible even as they proved highly manipulable.[175] When requiring the photographer's testimony became unsustainable, courts used a different tactic: they labeled the photo-

166. *See id.* at 29-30 (discussing "film bias").

167. *See* Deirdre Carmody, *Time Responds to Criticism over Simpson Cover*, N.Y. TIMES (June 25, 1994), http://www.nytimes.com/1994/06/25/us/time-responds-to-criticism-over-simpson-cover.html [http://perma.cc/HP4Q-BCV4] (discussing the criticism and debate surrounding Time Magazine's cover photograph of O.J. Simpson, which had been "doctored" to look darker).

168. G. Daniel Lassiter et al., *Videotaped Interrogations and Confessions: A Simple Change in Camera Perspective Alters Verdicts in Simulated Trials*, 87 J. APPLIED PSYCHOL. 867, 867 (2002).

169. Benjamin V. Madison III, *Seeing Can Be Deceiving: Photographic Evidence in a Visual Age—How Much Weight Does It Deserve?*, 25 WM. & MARY L. REV. 705, 720 (1984).

170. *See id.* at 717-18 (citing Johnson v. State, 636 P.2d 47 (Alaska 1981)).

171. *See* Silbey, *supra* note 164, at 39-40.

172. *See* Madison, *supra* note 169, at 730 (citing Powell v. Indus. Comm'n, 418 P.2d 602 (Ariz. Ct. App. 1966)).

173. *Id.* at 722.

174. Mnookin, *supra* note 155, at 39-40.

175. *Id.* at 57-58.

graph as merely "demonstrative" of a witness's testimony about an event, rather than as substantive evidence in its own right, thereby "demot[ing] the photograph from the nearly irrefutable to the merely illustrative."[176]

But that fiction eventually collapsed as well. Photographs are now, along with films and x-ray images, "readily accept[ed]"[177] in most American jurisdictions without an accompanying human witness, under a so-called "silent witness" theory.[178] In any event, many photographic systems—such as surveillance cameras, red light cameras, and ATM video footage—are now automatic and collect images without a person behind the camera. Courts still require authentication to prove the photograph depicts what the proponent says it depicts, but such proof can typically be from the photograph alone[179] under the theory that it "speaks for itself."[180] Because photographs are considered neither mere appendages to human testimony nor "testimony" under the law of evidence, they are caught in a netherworld along with other machine conveyances and underscrutinized for the presence of black box dangers.[181]

2. *Basic Scientific Instruments*

For well over a century, courts have implicitly acknowledged the credibility-dependent nature of the measurements of instruments, basing their admission on characteristics likely to minimize black box dangers. By the mid-nineteenth century, there existed a "public depot of scientific instruments" for "commercial" and "nautical purposes."[182] Many such instruments made their way into English and American courtrooms, including clocks, watches, thermometers, barometers, pedometers, wind speed measures, and "a variety of other ingen-

---

176. *Id.* at 58.

177. Madison, *supra* note 169, at 714.

178. *See* Tracy Bateman Farrell, Annotation, *Construction and Application of Silent Witness Theory*, 116 A.L.R. 5th 373 (2004).

179. *See, e.g.*, Madison, *supra* note 169, at 736 ("Several courts have suggested that the silent witness theory, which would treat X-rays as self-authenticating evidence, is the best theory for admitting X-rays into evidence.").

180. Farrell, *supra* note 178, § 3.

181. *See* Madison, *supra* note 169, at 714-15 (noting that courts now have "substantial faith [in] the reliability of the photographic process"); Silbey, *supra* note 164, at 26 & n.58 (arguing that film presents testimonial risks and should be examined more critically).

182. 3 LEVI WOODBURY, WRITINGS OF LEVI WOODBURY, LL. D: POLITICAL, JUDICIAL AND LITERARY 38 (1852).

ious contrivances for detecting different matters."[183] Although litigants would occasionally insist that an instrument's measurement was inaccurate,[184] courts afforded scientific instruments a presumption of correctness "akin to" the usual course of business hearsay exception for mercantile records offered for their truth.[185] John Henry Wigmore, in his influential 1904 treatise, placed his discussion of "scientific instruments" under the rubric of hearsay rather than physical evidence, noting that the accuracy of instruments' conveyances depends on the credibility of others:

> The use of *scientific instruments, apparatus, and calculating-tables*, involves to some extent a dependence on the statements of other persons, even of anonymous observers. Yet, on the one hand, it is not feasible for the scientific man to test every instrument himself; while, on the other hand, he finds that practically the standard methods are sufficiently to be trusted . . . . The adequacy of knowledge thus gained is recognized for a variety of standard instruments.[186]

The 1899 edition of Simon Greenleaf's evidence treatise similarly discussed scientific instruments in the hearsay context: in noting that "an element of hearsay may enter into a person's sources of belief," he used examples such as "reckoning by a counting-machine."[187] Relying on instruments' regular production and use, modern courts often take "judicial notice" of their readings,

---

183. 1 JOHN PITT TAYLOR, A TREATISE ON THE LAW OF EVIDENCE, AS ADMINISTERED IN ENGLAND AND IRELAND; WITH ILLUSTRATIONS FROM THE AMERICAN AND OTHER FOREIGN LAWS § 148, at 185 (6th ed. 1872). Taylor's description reflects a broader instrument fetishism, particularly among royal families, that motivated the invention of, and solidified the epistemic authority of, many astronomical and mathematical devices. *See* MARY POOVEY, A HISTORY OF THE MODERN FACT: PROBLEMS OF KNOWLEDGE IN THE SCIENCES OF WEALTH AND SOCIETY 138-41 (1998).

184. *See, e.g.*, *In re* More's Estate, 121 Cal. 609, 616 (1898) (addressing a litigant's claim that a sheep-counting registering machine used by plaintiff to count the sheep returned by a lessee at the end of his lease was "unreliable"); Hatcher v. Dunn, 71 N.W. 343 (Iowa 1897) (addressing the plaintiff's argument that a thermometer used by a state inspector in certifying lamp oil as safe may have been faulty, after oil exploded at a temperature that was within an allegedly safe range).

185. TAYLOR, *supra* note 183, § 148, at 185.

186. 1 WIGMORE, *supra* note 50, § 665, at 1072.

187. 1 SIMON GREENLEAF, A TREATISE ON THE LAW OF EVIDENCE § 430, at 531 (16th ed. 1899).

without further foundation, on grounds that their accuracy is beyond reasonable dispute.[188]

As the presumption of correctness reflects, most basic scientific instruments are simple, transparent in terms of their design and process, not sensitive to human input error, and regularly made for a nonlitigative purpose. Yet as Part I made clear, even well-designed, simple, transparent instruments are still susceptible to errors of articulation when they have old batteries or worn markings, or to inferential errors based on an operator's placement decision. And for some instruments, like the sextant, accurate output largely depends on inputter and operator skill.[189] These potential flaws do not suggest the measurements of such instruments should be excluded, but that lawmakers should consider which operation protocols, impeachment mechanisms, and other safeguards sufficiently empower jurors to assess instrument credibility.

3. Computerized Business Records

Beginning in the mid-1960s, American courts faced litigation over the admissibility of computer records kept or created in the regular course of business.[190] While some computer records were "conduits" storing data inputted by humans, others were information generated by the computer as a source.[191] Most federal courts did not observe this distinction and instead, by the mid-1990s, treated all computer records as requiring a foundation under a hearsay exception,[192] perhaps bolstered by an oft-cited 1974 article opining that

---

188. *See, e.g.*, Ball v. LeBlanc, 792 F.3d 584, 590-91 (5th Cir. 2015) (taking judicial notice of temperature and heat index readings in a habeas corpus case brought by a prisoner).

189. *See, e.g.*, *Removing Error*, OCEAN NAVIGATOR (Jan. 1, 2003), http://www.oceannavigator.com/January-February-2003/Removing-Error [http://perma.cc/AM9N-YFC5] (noting that a "sextant can contribute at least seven possible sources of error to a sailor's quest for his position at sea," based on a failure to properly calibrate and use the instrument).

190. *See generally* FED. R. EVID. 901(b)(9) advisory committee's note to 1972 proposed rules (citing cases from the 1960s in which businesses used computers to store and sort data); Wolfson, *supra* note 23, at 154 n.20 (citing cases).

191. As one state court explained, such output "represents only the by-product of a machine operation which uses for its input 'statements' entered into the machine by out of court declarants," while the latter is the result "of the computer's internal operations . . . [and] does not represent the output of statements placed into the computer by out of court declarants." State v. Armstead, 432 So.2d 837, 839-40 (La. 1983).

192. *See, e.g.*, United States v. Blackburn, 992 F.2d 666, 672 (7th Cir. 1993) (holding that printout results of an automatic "lensometer" test on a pair of eyeglasses found at a robbery scene were admissible, but only under the federal residual hearsay exception). *See generally*

"[c]omputer-generated evidence will inevitably be hearsay."[193] These courts, like nineteenth-century courts facing the measurements of instruments, were rightly concerned about the sensitivity of computer-generated records to human design, input, and operator error. But their insistence upon regulating such records through a hearsay model had little grounding in law or logic.[194]

As more courts recognize both that computer-generated information is not hearsay and that it might still be inaccurate, some have looked to Federal Rule 901(b)(9) and its state analogs[195] for guidance. A provision in Rule 901(b)(9) allows proponents to authenticate the results of a "process or system" by "describing [the] process or system" used to produce the result and showing it "produces an accurate result."[196] The rule, proposed in 1968, responded directly to computerized business records.[197] Its original language provided, much like other traditional authentication rules, that a proponent prove that a system result "fairly represents or reproduces the facts which the process or system purports to represent, or reproduce."[198] But Judge Weinstein suggested adding the word "accurate" to the language,[199] meaning that proponents of machine processes now have a choice between authenticating the result through proof that the process produces an accurate result and authenticating it through other means. For computerized business records, the authentication requirement of

Wolfson, *supra* note 23, at 155-56 (noting that the vast majority of federal and state courts at the time treated computerized records as hearsay requiring a foundation as a business or public record to be admissible).

193. Jerome J. Roberts, *A Practitioner's Primer on Computer-Generated Evidence,* 41 U. CHI. L. REV. 254, 272 (1974).

194. *See generally* Wolfson, *supra* note 23 (criticizing American courts for treating computer-generated business records as hearsay).

195. *See, e.g.*, NEB. REV. STAT. § 27-901(2)(i) (1975). Canada also treats computer-generated records as "real evidence" subject to evidence about the "accuracy and integrity of the process employed." R. v. McCulloch, 1992 CarswellBC 2586, ¶ 18 (Can.) (WL).

196. FED. R. EVID. 901(b)(9).

197. All the cases cited in the advisory committee's notes to 901(b)(9) are cases from the 1960s involving tabulating machine results made during the regular course of a commercial business. *See* Merrick v. United States Rubber Co., 440 P.2d 314 (Ariz. App. 1968) (electronic accounting equipment); State v. Veres, 436 P.2d 629 (Ariz. App. 1968) (bank records on encoding machines); Transp. Indemnity Co. v. Seib, 132 N.W.2d 871 (Neb. 1965) (business records on tabulating machine).

198. ADVISORY COMM. FOR THE FED. RULES OF EVIDENCE, MINUTES 39 (Dec. 10, 1968).

199. Judge Weinstein suggested replacing the "fairly represents" language with a showing that the "result is accurate." *Id.*

Rule 901(b)(9) may screen clearly unreliable processes,[200] although as Part III makes clear, such records—like all machine conveyances—should also be open to impeachment and other scrutiny that provides the factfinder with additional context.

4. Litigation-Related Gadgetry and Software

Unlike the measurements of basic instruments and computerized business records, some machine-generated data are created specifically for civil or criminal litigation, motivating humans to design, input, and operate the machine to produce information favorable to the proponent.

A concern about this type of litigation-related bias—and an influential 1976 Second Circuit dissenting opinion expressing such concern—may have influenced courts from the 1970s to the early 2000s to treat computer-generated records as hearsay.[201] In a contract dispute between an inventor and a patent assignee, Singer Company, the inventor offered the conclusion of a proprietary computer program that an anti-skid automotive technology was capable of being perfected by Singer for sale.[202] Singer claimed the inventor's refusal to disclose the "underlying data and theorems employed in these simulations in advance of trial" left the company without a fair and adequate opportunity to cross-examine the inventor's expert witnesses.[203] The majority concluded Singer had enough fodder to cross-examine the experts who relied on the program, without learning more about the program itself.[204]

In dissent, Judge Van Graafeiland declared he was "not prepared to accept the product of a computer as the equivalent of Holy Writ."[205] Instead, "[w]here . . . a computer is programmed to produce information specifically for purposes of litigation," the product should be subject to greater scrutiny.[206] He suggested that the party introducing such information should have to dis-

---

200. Some 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]." *See, e.g.*, State v. Swinton, 847 A.2d 921, 942 (Conn. 2004).

201. *See* Wolfson, *supra* note 23, at 155-56 (suggesting that many courts followed the dissent).

202. Perma Research & Dev. v. Singer Co., 542 F.2d 111, 115 (2d Cir. 1976).

203. *Id.*

204. *Id.*

205. *Id.* at 121 (Van Graafeiland, J., dissenting).

206. *Id.* at 125.

close the computer "program" before trial to the opposing party, so that the party has the "opportunity to examine and test the inputs, program and outputs prior to trial."[207] Ultimately, the judge insisted, where a party's "entire case rests upon the accuracy of its computerized calculations," judges should "subject such computations to the searching light of full adversary examination."[208] A court in the 1980s similarly admitted a program called "Applecrash," which estimated the likely speed of a car during a collision,[209] rejecting the opponent's arguments for pretrial disclosure of the program's processes on grounds that cross-examination of the human expert who relied on the program was sufficient.[210]

More recently, courts have ruled on the reliability of litigation-related, computer-generated conclusions that form the basis of human expert testimony. Courts tend to admit such evidence so long as validation studies prove the reliability or general acceptance (under *Daubert* or *Frye*, respectively) of the program's methodology and the opponent can cross-examine the human expert.[211] In Part III, I explore the limitations of existing reliability-based admissibility rules as a means of testing machine credibility. Meanwhile, courts have admitted other nonscientific algorithms with no *Daubert* scrutiny at all.[212]

In criminal cases, courts have also tended to subject the conveyances of gadgets and software created for law enforcement purposes to reliability

---

207. *Id.* (citation omitted).

208. *Id.* at 126.

209. Commonwealth v. Klinghoffer, 564 A.2d 1240, 1241 (Penn. 1989) (Larsen, J., dissenting) (relying on *Perma* dissent).

210. *Id.* at 1242 (arguing the court was wrong to treat the cross-examination of the expert as sufficient for admissibility of the program, without also considering pretrial discovery of the program's information and data).

211. *See, e.g.*, *In re* Yamaha Motor Corp. Rhino ATV Prods. Liab. Litig., 816 F. Supp. 2d 442, 462-63 (W.D. Ky. 2011) (holding that computer analysis must pass the test of reliability and that cross-examination is an appropriate test of accuracy); Livingston v. Isuzu Motors, Ltd., 910 F. Supp. 1473, 1494-95 (D. Mont. 1995) (admitting a computer-generated accident-reconstruction opinion because it had been subject to peer review and "the theory behind the computer simulation ha[d] been tested"); Commercial Union Ins. Co. v. Boston Edison Co., 591 N.E.2d 165, 168 (Mass. 1992) (requiring proof that the computer's method is generally accepted).

212. *See* UMG Recordings, Inc. v. Lindor, 531 F. Supp. 2d 453, 457 (E.D.N.Y. 2007) (denying defendant's motion to exclude expert testimony, given that the expert's opinion was based on "objective data," and that the defendant was "free to use cross-examination" of the industry's expert to resolve any accuracy issues); Bratus et al., *supra* note 103, at 403-04 (criticizing the *Lindor* court for failing to better scrutinize the results of proprietary software harnessed by the recording industry to document allegedly illegal downloads from a user's computer).

tests,[213] but have routinely admitted them. In the early twentieth century, courts faced a wave of fact-detecting, "ingeniously contrived"[214] gadgets. The *Harvard Law Review* published a note in 1939 titled "Scientific Gadgets in the Law of Evidence," chronicling ABO typing, blood-alcohol testing, deception tests, filmic evidence, and fingerprint and ballistic analysis.[215] One scholar wrote in 1953 that the "whole psychological tone" of the new "scientific age" of the early twentieth century "embodie[d] an increasing reliance on gadgets."[216] Some of these gadgets explicitly conveyed information in symbolic output, and some were made expressly for law enforcement purposes. For example, radar guns and tachometers recorded car speed and were soon used in traffic prosecutions.[217] The Drunk-O-Meter, unveiled in 1938, and the Breathalyzer, unveiled in 1954, recorded the concentration of alcohol in deep lung air.[218]

While these analog gadgets were often uncomplicated in their construction,[219] they were sometimes maligned by judges and commentators in language suggesting concerns about black box dangers. The Breathalyzer, for example, was derided as "Dial-a-Drunk" because it forced a police officer to manually set a baseline before testing a suspect.[220] And judges, apparently expressing concern over the black box opacity of certain guilt-detecting gadgets, warned that both the radar gun and the Breathalyzer might usher in an era of

---

213. *Frye* itself might appear an exception, given that it rejected expert testimony based on the polygraph. Frye v. United States, 293 F. 1013, 1014 (D.C. Cir. 1923). But the polygraph itself simply measures physical phenomena like heart rate and blood pressure, measurements that were not in serious dispute. The court's concern appeared to be with the reliance on the polygraph by the examiner, William Moulton Marston, later the inventor of Wonder Woman. *See generally* Jill Lepore, *On Evidence: Proving* Frye *as a Matter of Law, Science, and History*, 124 YALE L.J. 1092 (2015) (exploring *Frye* as a case study in how and why law "hides" certain facts).

214. State v. Hunter, 68 A.2d 274, 275 (N.J. Super. Ct. App. Div. 1949) (describing the Drunk-O-Meter).

215. Notes and Legislation, *Scientific Gadgets in the Law of Evidence*, 53 HARV. L. REV. 285 (1939).

216. Dillard S. Gardner, *Breath-Tests for Alcohol: A Sampling Study of Mechanical Evidence*, 31 TEX. L. REV. 289, 290 (1953).

217. *See, e.g.*, People v. Offermann, 125 N.Y.S.2d 179 (Sup. Ct. 1953) (radar gun).

218. *See* Andrea Roth, *The Uneasy Case for Marijuana as Chemical Impairment Under a Science-Based Jurisprudence of Dangerousness*, 103 CALIF. L. REV. 841, 843, 861 (2015).

219. The Breathalyzer, for example, was invented by a police photographer with a high school education, who described the machine as "so amazingly simple—two photo cells, two filters, a device for collecting a breath sample, [and] about six wires." BARRON H. LERNER, ONE FOR THE ROAD: DRUNK DRIVING SINCE 1900, at 48-49 (2011).

220. Roth, *supra* note 218, at 861.

"push button justice."[221] Courts still occasionally reject a particular gadget or program as being unreliable enough to exclude under *Frye* or *Daubert*,[222] but such cases are few and far between, particularly now that breath-alcohol testing is subject to so many front-end safeguards. Many states now limit the type of machines that can be used and enforce operation protocols to ensure accurate results.[223]

In subsequent decades, these gadgets have shifted from analog to digital forms, reducing certain aspects of their manipulability, but exhibiting a "creeping concealedness" in their opacity and complexity.[224] While the Drunk-O-Meter required a human to do the arithmetic necessary to translate its color test and scale-measured breath weight into blood-alcohol content,[225] modern breath-alcohol tests based on infrared and fuel cell technology offer a print-out report or digital screen reading.[226] Radar gun software and output,[227] as well as infrared spectrometers and gas chromatographs reporting drug levels in blood,[228] have also graduated to digitized, software-driven forms.

A number of other modern computer-driven sources of information, built in anticipation of law enforcement use, now exist, including stingray devices that can record incoming and outgoing phone numbers to a cell phone;[229] li-

---

221. *Offermann*, 125 N.Y.S.2d at 185; People v. Seger, 314 N.Y.S.2d 240, 245 (Amherst Cty. Ct. 1970) (Breathalyzer).

222. *See, e.g.*, Reed v. State, 391 A.2d 364, 377 (Md. 1978) (excluding spectrograph voice comparison results under *Frye*); Alan Johnson, *Judge Finds Breathalyzer Not Scientifically Reliable*, COLUMBUS DISPATCH (Aug. 22, 2013), http://www.dispatch.com/content/stories/local/2013/08/22/judge-finds-breathalyzer-not-scientifically-reliable.html [http://perma.cc/V527-T8G9].

223. *See* Roth, *supra* note 13, at 1298 & n.319.

224. Matthew B. Crawford, *Shop Class as Soulcraft*, 13 NEW ATLANTIS 7, 7 (Summer 2006) (describing new car engines); *see also id.* ("Lift the hood on some new cars now . . . and the engine appears a bit like the shimmering, featureless obelisk that so enthralled the cavemen in the opening scene of the movie *2001: A Space Odyssey*. Essentially, there is another hood under the hood.").

225. *See* R. N. Harger, *"Debunking" the Drunkometer*, 40 J. CRIM. L. & CRIMINOLOGY 497, 498 (1950).

226. *See, e.g.*, People v. Miller, 125 Cal. Rptr. 341, 342 (Ct. App. 1975); Roth, *supra* note 13, at 1271.

227. *See, e.g.*, SPEEDCAM AI, http://www.raserabwehr.de [http://perma.cc/8FU2-FDKM].

228. *See, e.g.*, People v. Lopez, 286 P.2d 469, 472 (Cal. 2012).

229. Kim Zetter, *Turns Out Police Stingray Spy Tools Can Indeed Record Calls*, WIRED (Oct. 28, 2015), http://www.wired.com/2015/10/stingray-government-spy-tools-can-record-calls-new-documents-confirm [http://perma.cc/X2AU-R827]. The Department of Justice represents that stingrays are currently used only to simulate cell sites and identify or locate particular phones. *See Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology*,

cense plate readers;[230] graphs of DNA test runs, purporting to show which genetic markers or "alleles" are present in a sample;[231] red-light camera time-stamp data;[232] address logs purporting to list IP addresses of users who have visited child pornography websites;[233] database-driven computer reports of the closest handful of matching archived records to an inputted latent print or ballistic image from a crime scene;[234] machine-learning crime-detecting programs;[235] drug identification software that can identify particular cutting agents used, which might lead investigators to a particular dealer;[236] and arson investigation software that offers an "answer" to whether debris suggests arson.[237] And a number of software programs now exist that offer a "score," based on several inputted variables, that represents the subject's future danger-

U.S. DEP'T JUST., http://www.justice.gov/opa/file/767321/download [http://perma.cc/EX44-WJ7J].

230. Kaveh Waddell, *How License-Plate Readers Have Helped Police and Lenders Target the Poor*, ATLANTIC (Apr. 22, 2016), http://www.theatlantic.com/technology/archive/2016/04/how-license-plate-readers-have-helped-police-and-lenders-target-the-poor/479436 [http://perma.cc/CN58-3794].

231. In forensic DNA analysis, analysts focus on locations, or "loci," along the subject's genetic strand that are highly variable among humans. At each location, they count how many times a particular genetic code repeats in a row (e.g., ACCG). The number of these Short Tandem Repeats (STRs) is the "allele" one has at that location. We all have two alleles at each locus; one inherited from each parent. *See* Erin Murphy, *The Art in the Science of DNA: A Layperson's Guide to the Subjectivity Inherent in Forensic DNA Typing*, 58 EMORY L.J. 489, 495-96 (2008); *see also* People v. Steppe, 152 Cal. Rptr. 3d 827, 833-34 (Ct. App. 2013) (holding that "raw data" from DNA analysis did not implicate the Confrontation Clause).

232. *See, e.g.*, People v. Goldsmith, 326 P.3d 239, 249-50 (Cal. 2014).

233. *See, e.g.*, John Robertson, Affidavit in Support of Application for a Search Warrant at 11-12, *In re* An Application for a Search Warrant for: The Premises Known and Described as [redacted] Brooklyn, NY 11211, No. 15-M-534 (E.D.N.Y. June 10, 2015).

234. *See* Simon A. Cole et al., *Beyond the Individuality of Fingerprints: A Measure of Simulated Computer Latent Print Source Attribution Accuracy*, 7 LAW PROBABILITY & RISK 165, 166 (2008) (explaining how the Automated Fingerprint Identification Systems database returns several "candidate" prints to the analyst).

235. *See supra* text accompanying notes 121-126.

236. *See, e.g.*, *Innovative Solutions for Drug Identification*, CENTICE (2014), www.centice.com/product-overview [http://perma.cc/UY7E-USXL].

237. *See, e.g.*, Bev Betkowski, *Computer Program Could Help Solve Arson Cases*, FORENSIC MAG. (Apr. 29, 2014, 1:13 PM), http://www.forensicmag.com/news/2014/04/computer-program-could-help-solve-arson-cases [http://perma.cc/98JS-AQMF].

ousness for purposes of criminal sentencing, parole, and civil commitment determinations.[238] Most of these programs are proprietary.[239]

In particular, complex proprietary software has dramatically affected criminal cases involving DNA mixture interpretation. DNA has revolutionized criminal trials and is now ubiquitous as a means of forensic identification.[240] But while some DNA samples comprise a large amount of a single person's DNA and are relatively easy to analyze, other samples contain mixed, low-quantity, or degraded DNA. Drawing inferences about the number and identity of contributors in such complex mixtures is a difficult business. As one DNA expert noted, "[I]f you show ten colleagues a mixture, you will probably end up with ten different answers."[241] Recognizing the inherent limitations of manual methods,[242] several companies now offer probabilistic genotyping software purporting to enhance the objectivity and accuracy of DNA mixture interpretation by automating the process both of calling "matches" and of generating a match statistic that explains the match's significance—that is, how many people in the population would have a DNA profile consistent with the mixture purely

238. *See* CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY 25 (2016) (noting that the "workings of a recidivism model are tucked away in algorithms, intelligible only to a tiny elite"); CHRISTOPHER SLOBOGIN, PROVING THE UNPROVABLE: THE ROLE OF LAW, SCIENCE, AND SPECULATION IN ADJUDICATING CULPABILITY AND DANGEROUSNESS 101-14 (2007) (discussing use of actuarial instruments in informing or replacing expert assessments of culpability and future dangerousness).

239. *See, e.g.*, People v. Superior Court *ex rel.* Chubbs, No. B258569, 2015 WL 139069, at *8 (Cal. Ct. App. Jan. 9, 2015) (noting that DNA mixture interpretation software TrueAllele is proprietary); *In re* Source Code Evidentiary Hearings in Implied Consent Matters, 816 N.W.2d 525, 528 (Minn. 2012) (noting proprietary nature of breath-testing software); Order Denying Defendant's Motion to Suppress Evidence, United States v. Michaud, 2016 WL 337263, at *3 (W.D. Wash. Jan. 28, 2016) (noting that government malware used in child pornography investigation was proprietary); State v. Loomis, 881 N.W.2d 749, 753-54 (Wis. 2016) (denying litigants access to source code of actuarial instrument used in parole hearing); Scott Calvert & Luke Broadwater, *City in $2 Million Dispute with Xerox over Camera Tickets*, BALT. SUN (Apr. 24, 2013), http://articles.baltimoresun.com/2013-04-24/news/bs-md-xerox-dispute-20130424_1_brekford-corp-81-red-light-cameras-xerox-state [http://perma.cc/59HU-D3QE] (noting that Xerox refused to share software for a red-light camera system on the ground that the software was proprietary).

240. *See generally* MURPHY, *supra* note 119 (exploring the widespread use of DNA as evidence in criminal trials).

241. Chris Smith, *DNA's Identity Crisis*, S.F. MAG., Sept. 2008, at 80 (quoting British geneticist Peter Gill).

242. *See, e.g.*, Itiel E. Dror & Greg Hampikian, *Subjectivity and Bias in Forensic DNA Mixture Interpretation*, 51 SCI. & JUST. 204, 206-07 (2011) (demonstrating that cognitive bias may have infected human analysts' DNA mixture interpretations).

by chance. As one program designer put it, we now have a "computer that interprets DNA evidence."[243] These systems differ in terms of the assumptions embedded in their source code and the form their reported match statistics take.[244] Some developers have opened their source code to the public;[245] others, such as Cybergenetics's "TrueAllele" program and New Zealand DNA expert John Buckleton's "STRmix," have not.[246] Courts have nearly universally admitted the results of these programs over objection in *Frye/Daubert* litigation,[247] and in at least one case, a defendant used results to convince prosecutors to support vacating his conviction.[248]

In one recent case, two expert DNA systems returned contradictory results based on the same factual input. In 2011, a twelve-year-old boy in Potsdam, New York was tragically strangled to death in an apartment he shared with his mother. Police suspicion fell upon Nick Hillary, a former college soccer coach who had dated the mother and who was upset about their breakup a few

---

243. *See TrueAllele Casework Process Overview Video*, CYBERGENETICS at 0:04 (May 1, 2013), http://www.cybgen.com/systems/casework.shtml [http://perma.cc/6EFT-S3VX].

244. *See* discussion *infra* Section III.A.

245. *See, e.g.*, Keith Inman et al., *Lab Retriever: A Software Tool for Calculating Likelihood Ratios Incorporating a Probability of Drop-out for Forensic DNA Profiles*, 16 BMC BIOINFORMATICS 298 (2015) (adding open-access code to an existing program).

246. *See, e.g.*, Perlin Letter, *supra* note 127 (requesting that the FBI withdraw its sole-source contract for STRmix, initiate a competitive bid process, and contract with Cybergenetics's TrueAllele).

247. *See* John S. Hausman, *Lost Shoe Led to Landmark DNA Ruling—And Now, Nation's 1st Guilty Verdict*, MLIVE.COM, http://www.mlive.com/news/muskegon/index.ssf/2016/03/lost_shoe_led_to_landmark_dna.html [http://perma.cc/Z3QU-NTBD] (reporting a conviction in Michigan as the first in the United States to be based in part on the STRmix software after the defense contested its admissibility); *Trials*, CYBERGENETICS, http://www.cybgen.com/news/trials.shtml [http://perma.cc/V7K9-GQQ4] (listing 48 cases in which TrueAllele has been admitted). *But see* People v. Hillary, Decision & Order on DNA Analysis Admissibility, Indictment No. 2015-15 (N.Y. St. Lawrence Cty. Ct. Aug. 26, 2016), http://www.cybgen.com/information/newsroom/2016/aug/files/08-26-16_Decision_and_Order-DNA_Analysis_Admissibility.pdf [http://perma.cc/3TFA-8VA5] (excluding STRmix results under *Frye*); Shayna Jacobs, *Judge Tosses Out Two Types of DNA Evidence Used Regularly in Criminal Cases*, N.Y. DAILY NEWS (Jan. 5, 2015, 2:30 AM), http://www.nydailynews.com/new-york/nyc-crime/judge-tosses-types-dna-testing-article-1.2065795 [http://perma.cc/2NPH-2L6Z] (reporting a Brooklyn judge excluded results from low copy number DNA testing and Forensic Statistical Tool testing).

248. *See, e.g.*, *Man Released from Prison After DNA Clears Him of 1989 Rape*, CBS LOCAL CHI. (Apr. 25, 2016, 7:15 AM), http://chicago.cbslocal.com/2016/04/25/darryl-pinkins-cleared-rape-dna-evidence [http://perma.cc/B37M-TSG9] (reporting that TrueAllele was used to convince prosecutors to acquiesce in exoneration of a convicted rapist).

months earlier.[249] Another former boyfriend, a deputy sheriff who had been physically violent with the mother, was cleared of suspicion based on a video showing him walking a dog several blocks away minutes before the incident. Rumors that another child may have killed the boy were also dismissed by police early on.[250] Focusing on Hillary, police surreptitiously took his DNA from a coffee cup and the butt of a cigarette and compared it to dozens of samples from the scene and the boy's body and clothing, with no resulting match.[251] Nor did any DNA samples taken from Hillary's car, home, or clothing match the boy's DNA. But analysts could not determine whether Hillary might be a contributor to a DNA mixture found under the boy's fingernail. Seeking a more definitive opinion, police in 2013 sent the DNA data to Mark Perlin, the creator of "TrueAllele." In 2014, Perlin reported that "[t]he TrueAllele computer found no statistical support for a match" with Hillary.[252] A year later, a new district attorney—elected on a promise to find the killer[253]—had the DNA data analyzed through STRmix, which reported that Hillary was 300,000 times more likely than a random person to have contributed to the mixture.[254] In September 2016, a trial judge excluded the STRmix results under *Frye*,[255] and Hillary was subsequently acquitted.[256]

---

249. *See* Jesse McKinley, *Tensions Simmer as a Small Town Seeks Answers in a Boy's Killing*, N.Y. TIMES (Mar. 5, 2016), http://www.nytimes.com/2016/03/06/nyregion/murder-of-garrett-phillips-in-potsdam-new-york.html [http://perma.cc/S8RY-Q5PG].

250. *Id.*

251. *Id.*

252. W.T. Eckert, *Hillary Trial Slated for Aug. 1*, WATERTOWN DAILY TIMES (Mar. 3, 2016, 12:30 AM), http://www.watertowndailytimes.com/news05/hillary-trial-slated-for-aug-1-20160303 [http://perma.cc/FA5M-63EY].

253. McKinley, *supra* note 249.

254. People v. Hillary, Notice of Motion To Preclude, Indictment No. 2015-15 (N.Y. St. Lawrence Cty. Ct. May 31, 2016) [hereinafter Hillary *Frye* Motion], http://www.scribd.com/doc/314644253/Hillary-Frye-Motion [http://perma.cc/5BCL-CHAW].

255. *See* Decision & Order on DNA Analysis Admissibility, *supra* note 247. The judge concluded that STRmix has been developmentally validated and is generally accepted as reliable, but excluded the results in Hillary's case nonetheless. *Id.* at 7. The judge cited the fact that the state crime laboratory that generated the raw data used by STRmix's creator in the analysis had not yet conducted the internal validation studies that the New York State Commission on Forensic Science currently requires of any laboratory seeking to send data to STRmix for analysis. *Id.* at 5-7.

256. Jesse McKinley, *Oral Nicholas Hillary Acquitted in Potsdam Boy's Killing*, N.Y. TIMES (Sept. 28, 2016), http://www.nytimes.com/2016/09/29/nyregion/oral-nicholas-hillary-potsdam-murder-trial-garrett-phillips.html [http://perma.cc/QA3M-375L].

5. Other Complex Algorithms, Robots, and Advanced Artificial Intelligence

A host of other types of machine conveyances are routinely offered for their truth in court, sometimes to prove a criminal defendant's guilt. Many of these conveyances come from machines created for general purposes, not for litigation, and many of those machines are driven by proprietary software. Common examples include Event Data Record information;[257] automated telephone responses giving telephone number information;[258] Google Earth satellite imagery and GPS coordinates;[259] software-generated driving time estimates;[260] "Find my iPhone" features used to track phone theft;[261] and Fitbit data used to impeach an alleged rape victim's claim about being asleep at the time of an attack.[262] Other expert systems are now available and seem capable of being offered as evidence, such as those rendering medical diagnoses[263] and automated language analysis,[264] and mobile facial recognition technology and goggles offering real-time information about observed subjects.[265]

Perhaps the final frontier in law's reliance on machine conveyances of information is the full automation of the act of witnessing. The jump from having an expert system render an opinion to having a robot[266] or android deliver that opinion to a jury face-to-face does not seem particularly fanciful. As one blogger asked, "[I]s it far-fetched to imagine Watson's now-familiar blue ava-

---

257. *E.g.*, Commonwealth v. Safka, 95 A.3d 304, 308-09 (Pa. Super. Ct. 2014) (admitting such evidence under *Frye*, in part because of its admission in four other states).

258. *E.g.*, United States v. Linn, 880 F.2d 209, 216 (9th Cir. 1989).

259. *E.g.*, United States v. Lizarraga-Tirado, 789 F.3d 1107, 1109-10 (9th Cir. 2015).

260. *E.g.*, Jianniney v. State, 962 A.2d 229, 232 (Del. 2008).

261. *E.g.*, Pickett v. State, 112 A.3d 1078, 1090 (Md. Ct. Spec. App. 2015).

262. *See* Jacob Gershman, *Prosecutors Say Fitbit Device Exposed Fibbing in Rape Case*, WALL ST. J.: LAW BLOG (Apr. 21, 2016, 1:53 PM), http://blogs.wsj.com/law/2016/04/21/prosecutors-say-fitbit-device-exposed-fibbing-in-rape-case [http://perma.cc/8C82-KVFM].

263. *See, e.g.*, Jonathan Cohn, *The Robot Will See You Now*, ATLANTIC (March 2013), http://www.theatlantic.com/magazine/archive/2013/03/the-robot-will-see-you-now/309216 [http://perma.cc/QC5C-5TQ6] (discussing emerging technology, such as IBM's Watson supercomputer, that can be used to automate medicine).

264. *See, e.g.*, Rada Mihalcea & Carlo Strapparava, *The Lie Detector: Explorations in the Automatic Recognition of Deceptive Language*, PROC. OF THE ACL-IJCNLP CONF. SHORT PAPERS 309, 312 (2009).

265. *See* Natasha Singer, *Never Forgetting a Face*, N.Y. TIMES (May 17, 2014), http://www.nytimes.com/2014/05/18/technology/never-forgetting-a-face.html [http://perma.cc/HS8V-D4GB].

266. By "robot" I mean a "mechanical object[] that take[s] the world in, process[es] what [it] sense[s], and in turn act[s] upon the world." Calo, *supra* note 69, at 529.

tar someday sitting on the witness stand?"[267] Even IBM's senior vice president for legal and regulatory affairs has suggested that Watson might have a place in the courtroom as a real-time fact checker.[268] And at least one legal scholar has suggested that artificial intelligence play the role of a court-appointed witness under Federal Rule of Evidence 706 in giving counsel to judges during *Frye/Daubert* hearings.[269] Likewise, "robot police"[270] and robot security guards[271] are already in use and could presumably offer information, in a suppression hearing or at trial, about a suspect's observed behavior.

Whether created for litigation or general purpose, these complex systems raise accuracy issues not adequately addressed by existing evidence law. The only clear legal rules that apply to them are basic rules of relevance and undue prejudice, authentication rules like Federal Rule 901(b)(9) requiring that a process produce an accurate result, and *Daubert-Frye* reliability requirements for human expert testimony. But as machine conveyances become ever more sophisticated and relied upon, factfinders need more information and context to assess machine credibility.

III. TESTIMONIAL SAFEGUARDS FOR MACHINES

This Part offers a brief vision of new testimonial safeguards built for machine sources of information. It first considers credibility-testing mechanisms that the law of evidence could adopt, and then considers whether accusatory

267. Robert Ambrogi, *Could IBM's Watson Make Experts Obsolete?* (Apr. 1, 2011), http://www.ims-expertservices.com/bullseye/april-2011/could-ibm-s-watson-make-experts-obsolete [http://perma.cc/7VH4-P4Z6].

268. Robert C. Weber, *Why "Watson" Matters to Lawyers*, NAT'L L.J. (Feb. 14, 2011), http://www.nationallawjournal.com/id=1202481662966/Why-Watson-matters-to-lawyers [http://perma.cc/TH8S-PBMN]; *see also* Jacob Gershman, *Could Robots Replace Jurors?*, WALL ST. J.: LAW BLOG (Mar. 6, 2013, 1:30 PM), http://blogs.wsj.com/law/2013/03/06/could-robots-replace-jurors [http://perma.cc/MB5K-PUEK].

269. Pamela S. Katz, *Expert Robot: Using Artificial Intelligence To Assist Judges in Admitting Scientific Expert Testimony*, 24 ALB. L.J. SCI. & TECH. 1, 36 (2014).

270. *See, e.g.*, Elizabeth Joh, *Police Robots Need To Be Regulated To Avoid Potential Risks*, N.Y. TIMES (July 14, 2016), http://www.nytimes.com/roomfordebate/2016/07/14/what-ethics-should-guide-the-use-of-robots-in-policing/police-robots-need-to-be-regulated-to-avoid-potential-risks [http://perma.cc/7RG4-PWNP].

271. *See, e.g.*, Rachel Metz, *Rise of the Robot Security Guards*, MIT TECH. REV. (Nov. 13, 2014), http://www.technologyreview.com/s/532431/rise-of-the-robot-security-guards [http://perma.cc/B8J3-NYA3].

machine conveyances in criminal cases might implicate the dignitary and accuracy concerns underlying the Confrontation Clause.

A. Machine Credibility Testing

The purpose of credibility-testing mechanisms is not primarily to exclude unreliable evidence, but to give jurors the context they need to assess the reliability of evidence and come to the best decision.[272] Indeed, in the machine context, a generalized rule of exclusion like the hearsay rule would harm the fact-finding process, given the promise of mechanization as a means of combatting the biases of human testimony. With that in mind, this Section explores safeguards that would give jurors more context about a machine conveyance, without necessarily excluding the information as unreliable. In choosing whether to adopt such safeguards, lawmakers must consider issues of cost; efficiency; fairness; the likelihood that, without the safeguard, the jury will draw the wrong inference; and the likelihood that, with the safeguard, the jury will overestimate the value of the impeachment material and undervalue the evidence.

1. Front-End Design, Input, and Operation Protocols

The first means of both improving the accuracy of machine conveyances and producing contextual information helpful to juries is to develop better protocols for design, input, and operation. Front-end protocols are underused but not entirely absent in the context of human testimony: the New Jersey Supreme Court, for example, has recognized a number of front-end protocols that can prevent human bias in stationhouse eyewitness identifications.[273] In the machine context, states have imposed protocols most conspicuously for breath-alcohol tests, requiring that testers use an approved machine and follow procedures targeting practices shown to produce ambiguity due to misplacement

272. *See* Swift, *supra* note 32, at 1342-43 (arguing against a "categorical approach" to hearsay and in favor of a "foundation fact approach" that would offer the jury "a witness knowledgeable about the circumstances affecting the declarant's process of perceiving, remembering, and making a statement about a relevant event"); *cf.* Richard D. Friedman & Jeffrey L. Fisher, *The Frame of Reference and Other Problems*, 113 MICH. L. REV. FIRST IMPRESSIONS 43, 45 (2014) (arguing that the goal of confrontation is not to ensure reliability, but to "help the trier of fact make *accurate* findings out of an assemblage of evidence, much of which may be very unreliable").

273. State v. Henderson, 27 A.3d 872, 919-22 (N.J. 2011) (setting forth a "non-exhaustive list of system variables" that can help courts determine whether to hold a *Wade* hearing to determine the validity of the eyewitness identification process).

and input error.[274] Such requirements need not be a condition of admission; in the breath-alcohol context, the failure to adhere to testing and operation protocols goes to weight, not admissibility.[275] But breath-alcohol testing is an outlier in this respect, likely for reasons relating to the history of DUI jurisprudence and the political capital of DUI defendants;[276] other types of forensic testing are not yet regulated by such a regime of detailed state-imposed protocols.

Generally, the more complex, opaque, and litigation-driven a machine's processes, the more design protocols are helpful. First, it is difficult for the jury, through a facial examination of the assertion and through mere questioning of the source itself or herself, to determine the assertion's accuracy: protocols help here for the same reason they are helpful in the stationhouse eyewitness identification process. Second, and putting litigative motive aside, the chance for inadvertent miscodes or analytical overreaching will be greater in machines that are highly complex or that attempt to model complexity, like self-driving car technology or Google Earth.

A jurisdiction might therefore require any software-driven system used in litigation to be certified as having followed software industry standards in design and testing. Though these standards are readily available,[277] programmers typically do not adhere to them in designing litigation-related software and courts and legislatures do not use them as a condition of admission. One software expert affirmed that STRmix, a probabilistic genotyping program, had not been rigorously tested according to industry standards,[278] and the pro-

274. For example, California requires that technicians determine the accuracy of their instruments through a "periodic analysis" of a sample of "known alcohol concentration" to ensure that the instrument produces a result within "0.01 grams % of the true value," CAL. CODE REGS. tit. 17, § 1221.4(a)(2)(A) (2016), and that the technician who administers the test observe the subject for at least fifteen minutes without interruption before the test, to ensure that the subject has not belched or vomited, which might render the test result inaccurate as a reflection of residual mouth alcohol rather than the alcohol concentration of deep lung air, CAL. CODE REGS. tit. 17, § 1219.3 (2016). The federal government also prohibits states from using machines other than those approved by the National Highway Transportation Safety Administration. *See* Conforming Products List of Evidential Breath Alcohol Measurement Devices, 77 Fed. Reg. 35,747, 35,748 (June 14, 2012).

275. *See, e.g.*, People v. Adams, 131 Cal. Rptr. 190, 195 (Ct. App. 1976) (holding that a failure to follow calibration requirements for breath-alcohol equipment went only to weight).

276. *See generally* Roth, *supra* note 218 (discussing history of breath-alcohol testing and criminal DUI laws).

277. *See, e.g.*, Declaration of Nathaniel Adams at 2, People v. Hillary, Indictment No. 2015-15 (N.Y. St. Lawrence Cty. Ct. May 27, 2016) (citing several governing bodies that have promulgated industry standards for software development and testing).

278. *See id.* at 3.

gram's creators have had to disclose publicly multiple episodes of miscodes potentially affecting match statistics.[279] Critical errors were also found during review of source code in litigation over the Toyota Camry's unintentional acceleration problem.[280] A software expert who reviewed the source code of the "Alcotest 7110," a breath-alcohol machine used in New Jersey, found that the code would not pass industry standards for software development and testing. He documented 19,500 errors, nine of which he believed "could ultimately [a]ffect the breath alcohol reading."[281] A reviewing court found that such errors were not a reason to exclude results, in part because the expert could not say with "reasonable certainty" that the errors manifested in a false reading,[282] but the New Jersey Supreme Court did cite the errors in requiring modifications of the program for future use.[283] Exclusion aside, a more robust software testing requirement reduces the chance of misleading or false machine conveyances.

Even where software is well written to operationalize the intended method, the method itself might be biased in ways that could be avoided if the design process were less opaque. One scholar has advocated what he terms "adversarial design,"[284] a means of building models that itself is political, reflecting normative controversies and compromises. If the process of developing risk assessment tools, credit score algorithms, or genotyping software were itself more adversarial, with input from all sides of contentious debates, we would presumably see less tolerance for analytical biases and fewer variables that cor-

279. *See* STRmix, Final Report—Variation in STRmix Regarding Calculation of Expected Heights of Dropped Out Peaks at 1-2 (July 4, 2016) (on file with author) (acknowledging coding errors but noting that errors would only underestimate likelihood of contribution).

280. Transcript of Testimony of Michael Barr at 47-50, Bookout v. Toyota Motor Corp., No. CJ-2008-7969 (Okla. Dist. Oct. 14, 2013), http://www.safetyresearch.net/Library/Bookout_v_Toyota_Barr_REDACTED.pdf [http://perma.cc/N2KP-ZS7K] (noting numerous software errors leading to Toyota Camry unintended acceleration issue that were only apparent upon review of source code).

281. *See* Supplemental Findings and Conclusions of Remand Court at 11, State v. Chun, No. 58,879 (N.J. Dec. 14, 2005), http://www.judiciary.state.nj.us/pressrel/supplemental_opinion.pdf [http://perma.cc/N6ZB-VLCW].

282. *Id*.

283. *See* State v. Chun, 943 A.2d 114, 129-35 (N.J. 2008); *see also* Robert García, *"Garbage In, Gospel Out": Criminal Discovery, Computer Reliability, and the Constitution*, 38 UCLA L. REV. 1043, 1088 (1991) (citing GAO report finding deficiencies in software used by Customs Office to record license plates, and investigations of failures of IRS's computer system).

284. DISALVO, *supra* note 35, at 16 (noting the importance of "*mak[ing] ideas, beliefs, and capacities for action experientially accessible and known*" through a "*normative*" practice of design).

relate to race.[285] Because of extant biases and racial variables, courts and legislatures should consider requiring that software used in criminal trials and sentencings be publicly designed and open-source. Experts have proposed similar public solutions to other black box scenarios, such as the credit scoring system.[286] Public models would have the benefit of being "transparent" and "continuously updated, with both the assumptions and the conclusions clear for all to see."[287]

When algorithms are privately developed, a public advisory committee could still promulgate requirements related to key variables or assumptions. For example, programmers of probabilistic genotyping software should not be the ones to choose the level of uncertainty that prompts a system to declare a DNA mixture "inconclusive" as opposed to declaring someone a potential contributor,[288] or to choose their own estimate related to the frequency of certain phenomena, such as genetic markers or allelic drop-out. Developing such guidelines for the substance and scope of machine testimony would be analogous to the National Commission on Forensic Science's recent call for human experts to cease using the phrase "reasonable degree of scientific certainty."[289]

Programs that use machine-learning techniques might require their own set of protocols to promote accuracy. Data scientists have developed very different "evaluation metrics" to test the performance of machine-learning models depending on the potential problem being addressed. For example, testers might use a technique called "hold-out validation" to determine whether a "training set" of data used at the beginning of supervised learning is an appropriate set on which to train the machine.[290]

Beyond design, input and operation protocols may be important for machines particularly sensitive to case-specific human errors, from sextants to

---

285. *See, e.g.*, O'NEIL, *supra* note 238, at 207 ("For example, a model might be programmed to make sure that various ethnicities or income levels are represented within groups of voters or consumers.").

286. *See* PASQUALE, *supra* note 18, at 208; *see also* Chessman, *supra* note 16, at 183-84 (suggesting public funding of open-source software as an alternative to source code disclosure).

287. O'NEIL, *supra* note 238, at 27.

288. *See, e.g.*, Testimony of John Buckleton at 74-75, People v. Hillary, No. 2015-15 (N.Y. Sup. Ct. July 25, 2016) (STRmix creator explaining his choice to treat likelihood ratios between 0.001 and 1,000 as "inconclusive").

289. *See* Nat'l Comm'n on Forensic Sci., *Views of the Commission Regarding Use of the Term "Reasonable Scientific Certainty,"* U.S. DEP'T JUST. (2016), http://www.justice.gov/ncfs/file/839731/download [http://perma.cc/E9WE-FQZS].

290. ZHENG, *supra* note 123, at 4.

breath-testing devices. One means of encouraging and checking proper calibration is to require quality control and quality assurance logs, a practice currently part of most laboratory work. In the breath-testing context, the test results from each machine are automatically recorded and transmitted to an online data center, maintained and reviewed by the state.[291] In the context of entering GPS coordinates into Google Earth, like the officer in *Lizarraga-Tirado*, one could imagine documentation requirements as well. Another check on inputs and operation would be to allow an opponent's representative to be present for case-specific inputs and operation of a machine.

2. Pretrial Disclosure and Access

A number of pretrial disclosure and access rules already apply to human testimony. If the United States intends to use expert testimony in a criminal trial, it must disclose the qualifications of the expert and the bases and reasons for her testimony at the defendant's request.[292] The disclosure requirements in civil trials are even more onerous, requiring the expert to prepare a written report that includes the facts or data relied on.[293] Proponents must not discourage witnesses from speaking with the opponent before trial,[294] and in criminal trials, proponents must also disclose certain prior statements, or "Jencks material," of their witnesses after they testify.[295] These requirements offer notice of claims that might require preparation to rebut, the ability to speak with the witness before trial, and the ability to review prior statements for potential impeachment material.

Applying these principles to machine sources, a jurisdiction might require the proponent of a machine "expert"—a source that generates and conveys information helpful to the jury and beyond the jury's knowledge—to disclose the substance and basis of the machine's conclusion. As one DNA statistics expert told me, "I just want these expert systems to be subject to the same requirements as I am." A jurisdiction might therefore require access to the machine's source code, if a review of the code were deemed necessary to prepare a rebuttal of the machine's claims.

---

291. *See, e.g.*, Cincinnati v. Ilg, 21 N.E.3d 278, 280 (Ohio 2014).

292. *See* FED. R. CRIM. P. 16(a)(1)(G).

293. *See* FED. R. CIV. P. 26(a)(2)(B)(ii).

294. *See, e.g.*, Gregory v. United States, 369 F.2d 185, 188 (D.C. Cir. 1966) ("Both sides have an equal right, and should have an equal opportunity, to interview [state witnesses].").

295. *See, e.g.*, Jencks Act, 18 U.S.C. § 3500(b) (2012).

Creators of proprietary algorithms typically argue that the source code is a trade secret or that it is unnecessary to prepare a defense to the machine's conclusion so long as the opponent understands the "basic principles" underlying the machine's methods.[296] But it is not clear that trade secret doctrine would protect the source code of an algorithm used to convict or impose liability.[297] Moreover, validity of method and validity of software-driven implementation of method are not equivalent; as one group of researchers has argued, "[c]ommon implementation errors in programs . . . can be difficult to detect without access to source code."[298]

A jurisdiction might also require meaningful access to the machine before trial, so the opponent can both review the machine's code, if it is disclosed, and also input different assumptions and parameters into the machine—for example, those consistent with the opponent's theory of the case—to see what the machine then reports. TrueAllele offers access to its program to criminal defendants, with certain restrictions, but only for a limited time and without the source code.[299] This sort of "black box tinkering" allows users to "confront" the code "with different scenarios," thus "reveal[ing] the blueprints of its decision-making process,"[300] but it also approximates the process of posing a hypothetical to an expert for purposes of preparing cross-examination related to the opponent's theory. Indeed, the ability to tinker might be just as important as access to source code. Data science scholars have written about the limits of

296. *See, e.g.*, State's Response to Defense Motion To Compel at 19, State v. Fair, No. 10-1-09274-5 (Wash. Apr. 4, 2016), http://www.cybgen.com/information/newsroom/2016/apr/files/States-Response-to-Defense-Motion-to-Compel-TrueAllele-Source-Code.pdf [http://perma.cc/5V57-DH6U] ("Because the basic principles underlying the operation of the TrueAllele system have been published, it is inaccurate to describe TrueAllele as a 'black box' system."); Chessman, *supra* note 16, at 157 (noting that one rationale commonly given to protect source code is that it is a proprietary trade secret).

297. *See, e.g.*, Jencks v. United States, 353 U.S. 657, 671 (1957) (noting that the right of access to witnesses' prior statements should generally trump government claims of privilege); Chessman, *supra* note 16, at 157 (arguing that trade secrets doctrine does not protect source code in criminal cases). *See generally* Rebecca Wexler, Deadly Secrets: Intellectual Property in the Criminal Justice System (unpublished manuscript) (on file with author) (arguing that trade secrets doctrine should not apply in criminal cases).

298. Andrew Morin et al., *Shining Light into Black Boxes*, 336 SCI. 159 (2012). *See generally* Chessman, *supra* note 16 (arguing that access to source code is necessary to prevent or unearth a number of structural programming errors); Erin E. Kenneally, *Gatekeeping Out of the Box: Open Source Software as a MechanismTo Assess Reliability for Digital Evidence*, 6 VA. J.L. & TECH. 13 (2001) (same).

299. State's Response to Defense Motion To Compel, *supra* note 296, at 21.

300. Perel & Elkin-Koren, *supra* note 36, at 6.

transparency[301] and the promise of "reverse engineering" in understanding how inputs relate to outputs,[302] as well as the benefits of "crowdsourcing"[303] and "[r]uthless public scrutiny"[304] as means of testing models and algorithms for hidden biases and errors.

A jurisdiction could also require disclosure of "Jencks material" for machine sources.[305] If a party takes several photographs of an accident scene with different lenses and camera angles and cherry picks the best one to present in court, the remaining photographs should be disclosable as Jencks material of the camera. Similarly, the prosecution using probabilistic DNA software might be required to disclose the results of all prior runs of a machine of a particular sample under various assumptions and parameters.[306] Or consider a criminal case in which investigators find a latent fingerprint at a crime scene and run it through the federal fingerprint database system, which reports the top ten matching prints and allows a human analyst to declare if any is a likely match.[307] State officials generally refuse defense requests for access to the other reported near matches, notwithstanding arguments that these matches might prove exculpatory.[308]

---

301. *See, e.g.*, Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PA. L. REV. (forthcoming 2017), http://ssrn.com/abstract=2765268 [http://perma.cc/5X53-UWGX] (suggesting tools for algorithmic fairness that do not require access to source code).

302. Nicholas Diakopoulos, *Algorithmic Accountability Reporting: On the Investigation of Black Boxes*, TOW CTR. FOR DIG. JOURNALISM 30 (2013), http://www.nickdiakopoulos.com/wp-content/uploads/2011/07/Algorithmic-Accountability-Reporting_final.pdf [http://perma.cc/2KRX-QZWB].

303. O'NEIL, *supra* note 238, at 211 (calling for "crowdsourcing campaigns" to offer feedback on errors and biases in data sets and models).

304. Holly Doremus, *Listing Decisions Under the Endangered Species Act: Why Better Science Isn't Always Better Policy*, 75 WASH. U. L.Q. 1029, 1148 (1997).

305. At least two courts have held that computer output is not a "statement" for Jencks purposes. *See* United States v. Alexander, 789 F.2d 1046, 1049 (4th Cir. 1986) (holding that the Jencks Act does not apply to computer print-out of data used to conduct analysis later presented at trial); United States v. Dioguardi, 428 F.2d 1033, 1038 (2d Cir. 1970) (expressing concern over government's failure to disclose key facts about a computer, but rejecting defendant's Jencks argument out of hand).

306. Defense attorneys have reported anecdotally that the "case packets" they receive include only a partial disclosure of the results of runs, and that, in their view, a more complete picture would help to identify potential analytical flaws or "cherry picking" of data where it exists.

307. *See* Cole et al., *supra* note 234, at 166.

308. *See generally* Simon A. Cole, *More than Zero: Accounting for Error in Latent Fingerprint Identification*, 95 J. CRIM. L. & CRIMINOLOGY 985, 985-87 (2005) (discussing the case of Brandon

Likewise, a breath-alcohol machine's COBRA data, which has been helpful in unearthing errors with such machines,[309] might be more clearly disclosable and admissible for impeachment if the machine were treated as a witness. In a somewhat analogous case, the defendant in a 1975 tax fraud prosecution sought access to the IRS's computer system's previous reported lists of nonfilers, to determine whether any previous records were mistaken. The court did not dismiss the request out of hand, but ruled that the defendant had sufficient alternative means of testing the computer's accuracy, including his own expert's pretrial access to the IRS's data processing systems.[310]

3. Authentication and Reliability Requirements for Admissibility

Just as certain categories of human sources are particularly "risky,"[311] certain machine sources might be more risky than others because of their complexity, opacity, malleability, or partiality of purpose. Should a broad reliability-based rule of exclusion—akin to the hearsay rule—apply to machine conveyances that exhibit some combination of these traits? This Article does not advocate such a rule. The characteristics of machine conveyances do not lend themselves to categorical exclusion based on the lack of a particular characteristic or safeguard. While the hearsay rule focuses exclusively on human assertions rendered out of court, a categorical rule of exclusion for machines that focused on a particular level of complexity, opacity, manipulability, or litigative purpose would be difficult to draft and dramatically over- or underinclusive in terms of targeting truly "risky" machines. Even complex, opaque algorithms—like Google Earth—can offer highly probative, relatively accurate information that presumably should not be excluded from all trials simply because opponents lack access to, say, the source code. Indeed, a proponent of Google Earth results might reasonably be concerned that jurors will undervalue such results based on an opponent's speculative or anecdote-based arguments about

Mayfield, a man who was detained in connection with the 2004 Madrid bombing based on an erroneous latent fingerprint analysis).

309. Watson, *supra* note 40, at 381-82.

310. United States v. Liebert, 519 F.2d 542, 543, 550-51 (3d Cir. 1975); *see also* Turcotte v. Dir. of Revenue, 829 S.W.2d 494, 496 (Mo. Ct. App. 1992) (holding that the state's failure to file timely maintenance reports on a breath-alcohol machine did not "impeach the machine's accuracy"); 155 AM. JUR. 3D *Proof of Facts* § 455 (2016) (describing the admissibility of computerized business records).

311. Swift, *supra* note 29, at 518 (arguing that the hearsay rule's primary value is in excluding "[r]isky" declarants whose assertions would otherwise be admitted).

Google's unreliability. Moreover, the hearsay rule itself is highly criticized and lacking in empirical foundation.[312]

Some countries do, in fact, have admissibility requirements for machine-generated reports of information, but these requirements are limited. In the United Kingdom, a "representation . . . made otherwise than by a person" that "depends for its accuracy on information supplied (directly or indirectly) by a person" is not admissible in criminal cases without proof that "the information was accurate."[313] But computer evidence in the United Kingdom is otherwise presumed, "in the absence of evidence to the contrary," to be "in order," and commentators have lamented the inability to meaningfully rebut software-generated conclusions.[314] Still other countries rely mostly on judicial discretion in determining the accuracy of machine conveyances,[315] or allow such evidence so long as it is accompanied by a human expert.[316]

---

312. *See* Justin Sevier, *Popularizing Hearsay*, 104 GEO. L.J. 643, 648 (2016) (arguing that a common rationale for the hearsay rule—promoting decisional accuracy—is "empirically suspect and difficult to measure meaningfully"); David Alan Sklansky, *Hearsay's Last Hurrah*, 2009 SUP. CT. REV. 1 (criticizing the rule in its current form).

313. Criminal Justice Act 2003, c. 44, § 129(1) (Eng.). If the inputter's "purpose" is "to cause . . . a machine to operate on the basis that the matter is as stated," the machine output based on the statement is treated as hearsay, *id.* § 115(3), requiring the live testimony of the person inputting the statement, unless the statement is admissible under an exception or stipulation, or if the court "is satisfied that it is in the interests of justice" to admit the statement, *id.* § 114(1). The provision "does not affect the operation of the presumption that a mechanical device has been properly set or calibrated." *Id.* § 129(2).

314. *See, e.g.*, Stephen Mason, *Electronic Evidence, the Presumption of Reliability and Hearsay—A Proposal*, 177 CRIM. L. & JUST. WKLY. (Sept. 28, 2013), http://www.criminallawandjustice.co.uk/features/Electronic-Evidence-Presumption-Reliability-and-Hearsay---Proposal [http://perma.cc/4B9G-YLR7] (quoting *Evidence in Criminal Proceedings: Hearsay and Related Topics*, LAW COMMISSION 189 (1997), http://www.lawcom.gov.uk/wp-content/uploads/2015/03/lc245_Legislating_the_Criminal_Code_Evidence_in_Criminal_Proceedings.pdf [http://perma.cc/WU2H-CWFW]).

315. *See, e.g.*, David M. Paciocco, *Proof and Progress: Coping with the Law of Evidence in a Technological Age*, 11 CANADIAN J.L. & TECH. 181, 219 (2015).

316. *See, e.g.*, Tejas D. Karia, *Digital Evidence: An Indian Perspective*, 5 DIGITAL EVIDENCE & ELECTRONIC SIGNATURE L. REV. 214, 220 (2008) (noting that the Supreme Court of India admitted evidence from mobile phone records after concluding that "a cross-examination of the competent witness acquainted with the functioning of the computer during the relevant time and the manner in which the printouts of the call records were taken was sufficient to prove the call records"); Sa'id Mosteshar, *EO in the European Union: Legal Considerations*, *in* EVIDENCE FROM EARTH OBSERVATION SATELLITES: EMERGING LEGAL ISSUES 155, 158-59 (Ray Purdy & Denise Leung eds., 2013) (explaining that Germany has "no express laws" for evidence based on satellite data but may require expert testimony, and that Belgium and the Netherlands have no express laws, leaving admission to judicial discretion). India's only ex-

Of course, authentication rules should apply to machine sources: if output purports to be that of a particular machine, the jury should be able to rely on it as such. But authentication rules do not generally address the credibility or accuracy of a source.[317] As discussed in Part II, federal authentication rules and state analogs include a provision targeted at the type of computerized business records existing in 1968, allowing authentication of a result of a process or system by showing that the system produces an accurate result. But even this rule is not by its terms an accuracy requirement; it is simply one allowable means of authentication among many for computerized evidence.[318]

To the extent some courts have interpreted Federal Rule 901(b)(9) as requiring proof that any result of a mechanical process be "accurate" as a condition of admission, they have done so largely within the realm of computer simulations offering "expert" opinions, importing a *Daubert*-like reliability analysis.[319] I turn to this sort of reliability requirement for expert machines next. But it is worth noting that a general accuracy requirement, along the lines of 901(b)(9) or *Daubert*, might also be adopted to screen out unreliable machine processes that are not "expert," such as the lay observations of a poorly programmed robot security guard.

Rules requiring the scientific or technical methods of expert witnesses to be reliable and reliably applied should also extend to machine sources, at least those whose conveyances relate to matters beyond the ken of the jury.[320] *Daubert* and *Frye* technically do not apply to machine conclusions admitted without an accompanying human witness, although they could be modified to do so. Under current law, courts treat the machine as the method of a human expert, rather than as the expert itself, even when the expert is a "mere scrivener" for the machine's output.[321] As a result, any scrutiny of the machine's conclusion through *Daubert-Frye* comes through pretrial disclosure of the basis of the human expert's testimony, the pretrial admissibility hearing, and cross-examination of the human expert at trial. The machine itself is not subject to

press law related to machine assertions is a provision akin to Federal Rule of Evidence 901(b)(9) for electronic records. *See* Karia, *supra*.

317. *See, e.g.*, Paciocco, *supra* note 315, at 198 (explaining that authenticity "is about whether the electronic document is that which it is purported to be," not about whether the computer-generated evidence "associated with the document is accurate").

318. *See, e.g.*, Steven Goode, *The Admissibility of Electronic Evidence*, 29 REV. LITIG. 1, 33-34 (2009).

319. *See supra* note 200.

320. They would presumably not apply to lay machines like robot security guards.

321. *See supra* note 27 and accompanying text.

pretrial disclosure rules or impeachment, or any scrutiny equivalent to cross-examination.

A rule requiring that the machine itself follow a reliable, and reliably applied, method for reaching its conclusions would involve more scrutiny than a typical *Daubert-Frye* hearing currently offers. Most judges rely heavily on validation studies in concluding that a machine, whether it be the Intoxilyzer 8000 or TrueAllele, uses a generally reliable process to reach its result.[322] But validation studies alone, showing a low false positive rate or an expected relationship between input and output,[323] might be an inadequate basis upon which to declare a machine conveyance likely accurate. Predictive algorithms, for example, might suffer feedback loops that taint performance evaluation.[324] In the forensic identification context, a machine might be assumed reliable because its conveyances have not been proven to have ever led to a wrongful conviction, a problematic metric given the difficulty in proof.[325] Validation studies are also often conducted under idealized conditions unrepresentative of the challenges of real casework. In the DNA mixture context, precisely those mixtures deemed too challenging to resolve manually because of degradation or other issues are relegated to software to solve. Some software designers embrace this state of affairs; TrueAllele advertises that the company "always giv[es] an answer," even in the "most challenging" mixtures.[326] As one expert warned, "TrueAllele is being used on the most dangerous, least information-rich samples you encounter."[327]

---

322. *Daubert* itself calls for this focus on validation. *See* Daubert v. Merrill Dow Pharm., Inc., 509 U.S. 579, 592-93 (1993) (adopting the Popperian view of scientific validity based on "falsifiability") (quoting KARL POPPER, CONJECTURES AND REFUTATIONS: THE GROWTH OF SCIENTIFIC KNOWLEDGE 37 (5th ed. 1989)).

323. *See, e.g.*, Declaration of Joanne B. Sgueglia at 3, State v. Fair, No. 10-1-09274-5 (Wash. Sup. Ct. Apr. 1, 2016) (declaring TrueAllele reliable because, "[a]s data became more uncertain (low level template DNA and stochastic effects) the resulting [likelihood ratio] decreased accordingly. Real and mock casework scenarios, along with contrived mixtures, all gave expected results").

324. *See, e.g.*, O'NEIL, *supra* note 238, at 8-9 (explaining why predictive algorithms are self-justified through feedback loops that suggest the algorithm is successful).

325. *See, e.g.*, García, *supra* note 283, at 1107-08 (noting that in cases resulting in guilty pleas, "neither the defense nor the public will learn whether or how the government used computers against the defendant"); *cf.* O'NEIL, *supra* note 238, at 12 (noting a danger in using profits as a metric for algorithmic success in statistical systems used in business).

326. *See* Perlin Letter, *supra* note 127, at 3, 5.

327. Joe Palazzolo, *Defense Attorneys Demand Closer Look at Software Used To Detect Crime-Scene DNA*, WALL ST. J. (Nov. 18, 2015), http://www.wsj.com/articles/defense-attor

Because of its limitations, validation is a potentially incomplete method of ensuring the accuracy of machine reports in the form of statistical estimates and predictive scores:

> Laboratory procedures to measure a physical quantity such as a concentration can be validated by showing that the measured concentration consistently lies with an acceptable range of error relative to the true concentration. Such validation is infeasible for software aimed at computing a[] [likelihood ratio] because it has no underlying true value (no equivalent to a true concentration exists). The [likelihood ratio] expresses our uncertainty about an unknown event and depends on modeling assumptions that cannot be precisely verified in the context of noisy [crime scene profile] data.[328]

Effective validation studies would help determine whether a DNA expert system tends to falsely "include" subjects as a contributor to a mixture. But validation studies are much less informative, at least in their current state, for demonstrating how accurately (or inaccurately) a system predicts the likelihood of a subject's contribution.

Some experts have argued that access to the source code is the only meaningful way to determine whether a complex algorithm's method is both reliable and reliably applied.[329] This argument has intuitive appeal: even if an algorithm's variables and analytical assumptions are transparent and seemingly valid, the software is the means by which those assumptions are actually implemented by the machine, and should itself be validated.[330] Assuming there are no trade secret issues, access to source code seems obvious. On the other hand, transparency alone does not guarantee meaningful scrutiny of software.[331]

neys-demand-closer-look-at-software-used-to-detect-crime-scene-dna-1447842603 [http://perma.cc/YA6H-Y7UY].

328. Christopher D. Steele & David J. Balding, *Statistical Evaluation of Forensic DNA Profile Evidence*, 1 ANN. REV. STAT. & ITS APPLICATION 361, 380 (2014).

329. *See* Palazzolo, *supra* note 327 (quoting a defense expert, who reviewed the validation studies and testified to a need for access to the source code, as saying, "I don't know how [TrueAllele] arrives at its answers.").

330. *See* M.D. Coble et al., *DNA Commission of the International Society for Forensic Genetics: Recommendations on the Validation of Software Programs Performing Biostatistical Calculations for Forensic Genetics Applications*, 25 FORENSIC SCI. INT'L 191 (2016) (promulgating recommendations for software validation for DNA expert systems).

331. *See, e.g.*, Paul Ford, *What Should We Do About Big Data Leaks?*, NEW REPUBLIC (Apr. 6, 2016), http://newrepublic.com/article/132122/big-data-leaks [http://perma.cc/CFC7-2GZK] ("A transparent society is one that makes data not just available but usable.").

Source code is lengthy; TrueAllele has 170,000 lines of code.[332] If opponents (or the public) had unfettered and indefinite access to the software to tinker with it, and if the software were subject to robust front-end development and testing standards, access to the code might not be critical.[333] At the very least, software engineers should be deemed part of the "relevant scientific community" for determining whether a method is or is not generally accepted,[334] rather than judging the reliability of software based on whether it is "relied on within a community of experts."[335]

Notably, the two expert DNA systems that came to a different conclusion in the *Hillary* case 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. TrueAllele's creator recently criticized several aspects of STRmix's methodology in a strongly-worded letter to the FBI,[336] and cited on its website a defense motion in another case calling STRmix "foreign copycat software."[337] But without more information about how each program arrives at its match statistic, the opposing party has few tools to impeach the credibility of that conclusion. The tools for impeachment lie buried in the machine's black box.

4. Impeachment and Live Testimony

Whether a machine source survives an authenticity or reliability challenge, the opponent should still have an opportunity to impeach the source's credibility at trial. After all, even when an out-of-court human assertion is admitted under a reliability-based hearsay exception, the opponent can still impeach the declarant at trial using any of the declarant's prior inconsistent statements, evi-

---

332. *See* Palazzolo, *supra* note 327.

333. *But cf.* Kenneally, *supra* note 298, at 149 (arguing that proprietary software, while potentially highly reliable, is "inherently incompatible . . . with the tenets embodied in *Daubert*").

334. *See, e.g.*, Notice of Motion To Preclude at 26, People v. Hillary, No. 2015-15 (N.Y. Sup. Ct. May 31, 2016) (arguing that DNA scientists' testimony about reliability of a computer DNA sequencing program was incomplete without the testimony of computer scientists).

335. *See* 2 MCCORMICK ON EVIDENCE § 218 n.9 (Kenneth S. Brown et al. eds., 7th ed. 2013).

336. *See* Perlin Letter, *supra* note 127 (arguing that STRmix is overly subjective and otherwise flawed in several respects).

337. *See* Motion for *Frye* Hearing at 3, People v. Smith, No. 2015-042 (N.Y. Sup. Ct. 2015), http://www.cybgen.com/information/newsroom/2015/dec/Smith2015.pdf [http://perma.cc/Z37Z-6YWB].

dence of incapacity or bias, or character for dishonesty.[338] Once an opponent has access to the prior statements of a machine, the opponent could likewise impeach the machine's credibility, assuming a few modifications in existing impeachment statutes.[339]

Given the "distributed cognition" between man and technology that underlies machine conveyances, meaningful impeachment of the machine source might also involve scrutiny of the character or capacity of human programmers, inputters, and operators. Evidence that a human programmer has a character for dishonesty, for example, or might harbor bias because he has been paid money to develop a program for a particular litigant, is relevant to the likelihood of deception or bias in the machine's design.

Trial safeguards would not necessarily involve the live testimony of the programmer, although such a requirement might make sense depending on the black box dangers implicated. The United Kingdom's rule requiring accuracy of inputs, for example, requires the live testimony of the inputter when a machine representation relies on information provided by that inputter.[340] Other countries subject computer-generated conclusions to the hearsay rule if at any point a human intervened in the machine's processes for creating its record.[341] In South Africa, merely signing a document printed by a computer is enough to convert the document to hearsay.[342] But treating a machine conveyance as "hearsay" mistakenly ignores the machine's role in distributed cognition. Under a hearsay model, the live testimony of the human is deemed not only necessary, but *sufficient*, as a means of testing the machine's credibility. Cross-examination of the human expert might be insufficient to unearth the design, machine-learning, input, operator, or machine degradation errors that pervert the machine report upon which the expert relies. Accordingly, cross-

338. *See, e.g.*, FED. R. EVID. 806.

339. In the federal rules, some modes of impeachment are allowable only by statute. *See, e.g.*, FED. R. EVID. 608 (character for dishonesty); *id.* at 613, 801(d)(1)(A) (inconsistent statement). The federal rules also apply only to "witnesses," which the rules limit to "person[s]." *See id.* at 601.

340. *See* Mason, *supra* note 314.

341. *See, e.g.*, Gert Petrus van Tonder, The Admissibility and Evidential Weight of Electronic Evidence in South African Legal Proceedings: A Comparative Perspective (May 2013) (unpublished LL.M thesis, University of Western Cape), http://etd.uwc.ac.za/xmlui/bitstream/handle/11394/4833/VanTonder_gp_llm_law_2013.pdf [http://perma.cc/PTY6-SDG7].

342. *See* Fawzia Cassim, *Use of Electronic Evidence in South African Law*, *in* GLOBAL CRIMINOLOGY: CRIME AND VICTIMIZATION IN A GLOBALIZED ERA 85, 88-89 (K. Jaishankar & Natti Ronal eds., 2013).

examination does not seem to have helped in any of the wrongful conviction cases involving "junk science."[343]

The United Kingdom's solution of requiring the testimony of any inputter of information would, in the context of expert testimony, be a significant departure from American law, but one that might make sense. Under Federal Rule of Evidence 703 and its analogs, an expert can testify to an opinion, even if based on the hearsay of others.[344] A human expert, at least, can be cross-examined on her decision to rely on the assertions of others, and in a few jurisdictions, the declarants of such assertions, if they are deemed sufficiently "testimonial," must testify as a constitutional matter.[345] Most machines, on the other hand, cannot be cross-examined, and do not exercise judgment—independent of the programmer—in deciding what sorts of assertions to rely upon or not.

Looking further ahead, a jurisdiction might wish to require in-court cross-examination or out-of-court depositions of machine sources capable of answering questions posed to them, such as Watson-like expert systems. Requiring an oath and physical confrontation would presumably offer no further relevant context for the jury, unless a robot were programmed to sweat or exhibit other physical manifestations of deception on the witness stand. But allowing questioning of a machine before the jury might offer some of the same benefits as questioning human witnesses on the stand, in terms of resolving ambiguities in testimony, posing hypotheticals to an expert source, or pressing a source related to an inconsistency.

---

343. *See, e.g.*, Brandon L. Garrett, *The Constitutional Regulation of Forensic Evidence*, 73 WASH. & LEE L. REV. 1147, 1149 (2016) ("In an era of plea bargaining, the accuracy of forensic analysis depends far less on cross-examination at trial, and far more on sound lab techniques, full disclosure of strengths and limitations of forensic evidence to prosecutors and the defense, and careful litigation."); Sklansky, *supra* note 312, at 18.

344. FED. R. EVID. 703.

345. *See, e.g.*, People v. Goldstein, 843 N.E.2d 727, 730 (N.Y. 2005) (holding that statements of nontestifying witnesses, relied upon by a state psychiatrist in rendering an inculpatory opinion about the defendant's culpability, were subject to the Confrontation Clause). Four of the surviving eight Supreme Court Justices subscribe to the view that such assertions are offered for their truth, notwithstanding the legal fiction underlying Rule 703. *See* Williams v. Illinois, 132 S. Ct. 2221, 2264 (2012) (Kagan, Scalia, Ginsburg, and Sotomayor, JJ., dissenting); *id.* at 2255 (Thomas, J., concurring in the judgment).

5. Jury Instructions and Corroboration Requirements

As mentioned in Part I, certain forms of risky or routinely misanalyzed human assertions, such as accomplice testimony and confessions, are subject to special jury instructions. Nonetheless, jury instructions are an underused means of encouraging jurors not to under- or overvalue evidence they are prone to misunderstand or view with prejudice. With respect to machines, both dangers are present: juries might irrationally defer to the apparent objectivity of machines,[346] or reject machine sources because of an irrational mistrust of machines' apparent complexities, even when the sources are highly credible.[347]

Depending on the machine source, courts might directly inform juries about black box dangers. For example, where photographs are admitted as "silent witnesses," the court could instruct the jury about lens, angle, speed, placement, cameraperson bias, or other variables that might make the image insincere or ambiguous as a conveyor of information. Sometimes, these black box clues will not be available, or will be obvious to the jury from its own experience.[348] If not, the court should use jury instruction to educate the jury about the effect of these variables on the image they are assessing.[349] In short, courts should warn jurors not to "conflat[e] the realistic and the real" by treating a photograph as offering "direct access to reality"[350] rather than as offering the potentially biased or ambiguous result of a black box process.

One could also imagine corroboration requirements for certain machine sources, akin to requirements for confessions and accomplice testimony.[351] One

---

346. *See* Randolph A. Bain & Cynthia A. King, Comment, *Guidelines for the Admissibility of Evidence Generated by Computer for Purposes of Litigation*, 15 U.C. DAVIS L. REV. 951, 961 (1982) (noting that factfinders might be unduly "awed by computer technology").

347. *See, e.g.*, Jennifer L. Mnookin & Nancy West, *Theaters of Proof: Visual Evidence and the Law in* Call Northside 777, 13 YALE J.L. & HUMAN. 329, 357-58 (2001) (noting that a "jargon-filled" polygraph explanation "effectively distances viewers from the very machine they are apparently being encouraged to admire, instilling in them a mistrust of its scientific complexity").

348. For example, most jurors will be familiar with the fact that objects are "closer than they appear" in car rear-view mirrors.

349. *See* Madison, *supra* note 169, at 740 (arguing for jury instructions along these lines for phtographs). *See generally* Silbey, *supra* note 15 (suggesting a number of trial safeguards for explaining testimonial infirmities of images to factfinders).

350. Rebecca Tushnet, *Worth a Thousand Words: The Images of Copyright*, 125 HARV. L. REV. 683, 700-01 (2012).

351. Of course, the production of mechanical evidence might be easier for the prosecution than for the defense, and corroboration requirements might be crafted accordingly. *See generally*

way of dealing with the difficulty of validating the statistical estimates of law enforcement-elicited complex proprietary algorithms might be to require a second opinion from another machine.[352] In the *Hillary* case, a corroboration rule would have ended in a pretrial dismissal without having to endure a trial, because the machine experts did not agree on the defendant's inclusion as a likely contributor to the DNA mixture. Another rule might require additional corroborative evidence of guilt if machine conveyances are within a certain margin of error.[353] Such rules might be grounded either in concerns about accuracy, or in concerns about dignity or public legitimacy where a machine result is the only evidence of guilt.[354] In Europe, for example, the General Data Protection Regulation prohibits citizens from being "subject to a decision" that is "based solely on automated processing," if it has a legal or "similarly significant[]" effect on the citizen.[355]

My goal in cataloging these potential safeguards is not to insist upon particular rules. Instead, it is to catalog the reasonable possibilities, to make clear that any future regime of machine credibility testing should draw lessons from how human testimony has been regulated, and to offer fodder for future scholarly discourse about machine credibility.

B. Machine Confrontation

The foregoing Section discussed the extent to which certain types of machine evidence implicate credibility and thus might require credibility testing—analogous to human assertions—to promote decisional accuracy. This Section briefly discusses the related but different question of whether a machine source might ever be a "witness[] against" a criminal defendant under the Sixth

Saul Levmore & Ariel Porat, *Asymmetries and Incentives in Plea Bargaining and Evidence Production*, 122 YALE L.J. 690, 714 (2012) (noting asymmetries not in defense resources per se, but in the ability of the defense to incentivize or force the production of evidence).

352. *Cf.* CAL. CRIM. JURY INST'N 334 (prohibiting conviction based solely on testimony of an accomplice); David A. Moran, *In Defense of the* Corpus Delicti *Rule*, 64 OHIO ST. L.J. 817 (2003) (describing and defending the common law rule prohibiting conviction based solely on an uncorroborated confession).

353. *See, e.g.*, Paul A. Clark, *The Right To Challenge the Accuracy of Breath Test Results Under Alaska Law*, 30 ALASKA L. REV. 1, 44-45 (2013).

354. *See generally* Roth, *supra* note 13 (exploring public concern over "trial by machine").

355. Council Regulation 2016/679, art. 22, § 71, 2016 O.J. (L 119) 1, 14, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC [http://perma.cc/FL4V-9MA4]. I thank Tal Zarsky for alerting me to this provision.

Amendment's Confrontation Clause. A handful of scholars have addressed this question, and most conclude that machines themselves cannot be "witnesses"; only their human progenitors can be.[356] While the subject deserves Article-length treatment, this Section briefly takes it on and suggests that machine sources sometimes may, indeed, trigger a right of confrontation.

1. Machines as "Witnesses Against" a Criminal Defendant

The Confrontation Clause of the Sixth Amendment guarantees to a criminally accused the right to be "confronted with the witnesses against him."[357] The precise meaning of the term "witnesses" has been the subject of vigorous debate in the Supreme Court for decades. The doctrine that currently exists has been in place since 2004, but has been losing some ground and is unpopular among some scholars. This Section first takes what seems to be undisputed about the Clause's origins and purpose, and situates machines within that broad discussion. It then offers some thoughts on where machines fit within existing Supreme Court doctrine defining "witness."

One goal of the Confrontation Clause, if not its "ultimate goal," is to "ensure reliability of evidence."[358] A would-be accuser who is forced to take the oath, physically confront the person he is accusing, and endure cross-examination is less likely to make a false accusation. If he does make a false accusation, he is more likely to recant upon having to look the falsely accused in the eye. And the jury will have a better chance to assess the likelihood of falsehood if it can examine the declarant's physical demeanor in court.

But accusations made behind closed doors can also subvert the dignity of criminal procedure: there is "something deep in human nature that regards face-to-face confrontation between accused and accuser" not only as promoting accuracy but as "essential to a fair trial in a criminal prosecution."[359] The Supreme Court once quoted then-President Eisenhower with approval as declaring that "[i]n this country, if someone . . . accuses you, he must come up in

---

356. *See, e.g.*, Neville, *supra* note 64, at 10; Erick J. Poorbaugh, *Interfacing Your Accuser: Computerized Evidence and the Confrontation Clause Following* Melendez-Diaz, 23 REGENT U. L. REV. 213, 214-15 (2010). Another author concludes that the Clause would have to "evolve" to include machines, but is sympathetic to the view that it should. Sites, *supra* note 16, at 99-100.

357. U.S. CONST. amend. VI.

358. Crawford v. Washington, 541 U.S. 36, 61 (2004).

359. Coy v. Iowa, 487 U.S. 1012, 1017 (1988) (quoting Pointer v. Texas, 380 U.S. 400, 404 (1965)).

front. He cannot hide behind the shadow."[360] To "look me in the eye and say that"[361] is to recognize me as a full person, worthy of respect. Thus, accusers should not be able to "hide behind [a] shadow";[362] rather, they should "stand behind" the accusation.[363] This theme of responsibility for the truth of one's statement squares with epistemologists' "commitment" theory of assertion, which argues that "to assert a proposition is to make oneself responsible for its truth."[364] Such rhetoric has led scholars to acknowledge that, in addition to protecting decisional accuracy, "confrontation doctrine should protect the system's sense and appearance of fairness."[365]

One immediate target of the framers who ratified the Sixth Amendment was the centuries-old practice of using sworn affidavits of witnesses, which justices of the peace took during ex parte meetings in a "modestly formal setting, likely the [justice's] parlor,"[366] in lieu of live testimony against a defendant at trial.[367] While the justices did not necessarily intend for these affidavits to replace witness testimony at trial, the Crown began to use them for that purpose. Even if the justice questioned a witness in good faith, and even if the witness did not recognize the full accusatory import of her statements, the resulting affidavit often contained mistakes, ambiguities, omissions, questionable inferences, and a slant toward a particular version of events that could not be probed or corrected at trial.[368] Moreover, the defendant had no opportunity to look the witness in the eye as the witness rendered her accusation. Finally, the affidavits were sworn and had all the trappings of formality, which might have unduly swayed jurors.[369] Faced with such unconfrontable but impressive-looking affidavits, defendants stood little chance of disputing them, even though the documents suffered "hearsay dangers." The human affiants, while

---

360. *Id.* at 1018 (citation omitted).

361. *Id.*

362. *Id.*

363. Sherman J. Clark, *An Accuser-Obligation Approach to the Confrontation Clause*, 81 NEB. L. REV. 1258, 1268 (2003).

364. Charles Sanders Peirce, *Reason's Rules (c. 1902)*, *in* 5 THE COLLECTED PAPERS OF CHARLES SANDERS PEIRCE ¶ 538, ¶ 543 (Charles Hartshorne & Paul Weiss eds., 1958-1966).

365. Friedman, *supra* note 15, at 692 n.54.

366. Robert P. Mosteller, Crawford v. Washington*: Encouraging and Ensuring the Confrontation of Witnesses*, 39 U. RICH. L. REV. 511, 555-59 (2005).

367. *See* Crawford v. Washington, 541 U.S. 36, 45-46 (2004).

368. *Id.*

369. *See, e.g.*, Melendez-Diaz v. Massachusetts, 557 U.S. 305, 329 (2009) (Thomas, J., concurring).

not bearing witness in court, clearly served as "witnesses against" the accused for purposes of implicating a right of confrontation.[370]

The state's use of accusatory machine conveyances to prove a defendant's guilt seems to implicate many of the same dignitary and accuracy concerns underlying the framers' preoccupation with in-the-shadows accusations and ex parte affidavits. To be sure, a machine is not, as far as we now know, capable of taking moral responsibility for a statement, or of understanding the moral gravity of accusing someone of a crime. But people are capable of doing those things, and when they build a machine to do the job, something may be lost in terms of moral commitment, if the person who is morally or epistemically responsible for the accusation is not called to vouch for the accusation in court. The court that first labeled the radar gun "push button justice" akin to "push button war" spoke only eight years after Hiroshima.[371] Some view a "push button war" as threatening in part because it is easier to wage when one does not have to see the people one is killing.[372] Perhaps it is easier to accuse someone when one builds an algorithm to do so.

In turn, the more inscrutable a machine process, the more its accusatory conveyances threaten the dignity of the accused and the perceived legitimacy of the process. In Kafka's *In the Penal Colony*, a machine is programmed to inscribe on a condemned man's back the law corresponding to his offense, which ultimately tortures and kills him in the process.[373] Only one official is left who is willing to run the device, and Kafka emphasizes the sinister indecipherability of the machine's blueprints.[374] The polygraph, too, was mistrusted in part because of its inscrutability.[375] One commentator in 1955 wrote that "[t]he fear or distrust of lie detectors is in part due to the conception that the machine itself will become a 'witness.'"[376] A justice of the Oregon Supreme Court even articulated a "personhood" argument against the polygraph, reasoning that parties should

---

370. *Crawford*, 541 U.S. at 43-46. While many legal scholars criticize *Crawford*'s exclusive focus on "testimonial" hearsay, the fact that ex parte affidavits implicate the core concerns underlying the Clause is not disputed. *See* sources cited *infra* note 384.

371. People v. Offermann, 125 N.Y.S.2d 179, 185 (Sup. Ct. 1953).

372. *See, e.g.*, Colin Allen, *The Future of Moral Machines,* N.Y. TIMES: OPINIONATOR (Dec. 25, 2011, 5:30 PM), http://opinionator.blogs.nytimes.com/2011/12/25/the-future-of-moral-machines [http://perma.cc/D7QT-VE7K] (noting issues with "battlefield machines").

373. FRANZ KAFKA, IN THE PENAL COLONY 3 (Ian Johnston trans., CreateSpace 2014) (1919).

374. *Id.*

375. Mnookin & West, *supra* note 347, at 354-57.

376. James R. Richardson, *Scientific Evidence in the Law*, 44 KY. L.J. 277, 285 (1955).

be "treated as persons to be believed or disbelieved by their peers rather than as electrochemical systems to be certified as truthful or mendacious by a machine."[377] As one scholar of data science noted, "even when such models behave themselves, opacity can lead to a feeling of unfairness."[378]

Allowing the state to build or harness machines to render accusations, without also providing the defendant a constitutional right to test the credibility of those machine sources, resembles trial by ex parte affidavit. The conclusions of proprietary software created in anticipation of litigation replaces live human testimony at trial and obviates the state's need to put a human expert on the stand to explain her methods and inputs that prompted the accusatory conclusion. And like an affidavit taken by a justice of the peace, the accusatory output—particularly output from machines created by or under contract with the state—might be incomplete or implicitly biased, even if sincere or technically accurate. As one scholar put it, "raw data is an oxymoron"[379]: all machine output reflects human choices about input, just as a direct examination of a witness in a justice's parlor reflects choices about what questions to ask. Some "raw data" will be more helpful to the government's case than others. In the *Hillary* case, for example, the district attorney shopped around until she found an expert system that would include the suspect as a potential contributor to the DNA mixture.[380] Moreover, just as the Framers were concerned that factfinders would be unduly impressed by affidavits' trappings of formality, "computer[s] can package data in a very enticing manner."[381] The socially constructed authority of instruments, bordering on fetishism at various points in history, should raise the same concerns raised about affidavits.

To say that machines built for criminal accusation implicate the concerns underlying the Confrontation Clause is not to say that the programmer is the one true "declarant" of the machine's accusatory conveyance. After all, the justice of the peace was not the true declarant of an affiant's sworn testimony: the affiant's own testimonial infirmities were at stake. Nonetheless, the justice's role in creating and shaping the affidavit was relevant in viewing the affiant as a "witness" in need of confrontation. The "involvement of government officers in the production of testimonial evidence" presents particular "risk[s]" of

---

377. State v. Lyon, 744 P.2d 231, 240 (Or. 1987) (en banc) (Linde, J., concurring).

378. O'Neil, *supra* note 238, at 28.

379. *See generally* "Raw Data" Is an Oxymoron (Lisa Gitelman ed., 2013) (collecting essays exploring how the generation and interpretation of data is culturally determined).

380. *See supra* notes 249-256 and accompanying text.

381. Roberts, *supra* note 193, at 274.

abuse.[382] Perhaps these possibilities loomed large for Justice Goodwin Liu as he dissented from an opinion of the California Supreme Court stating that machines cannot be witnesses under the Clause:

> [A]s a result of ever more powerful technologies, our justice system has increasingly relied on ex parte computerized determinations of critical facts in criminal proceedings—determinations once made by human beings. A crime lab's reliance on gas chromatography may be a marked improvement over less accurate or more subjective methods of determining blood-alcohol levels. The allure of such technology is its infallibility, its precision, its incorruptibility. But I wonder if that allure should prompt us to remain alert to constitutional concerns, lest we gradually *recreate through machines instead of magistrates the civil law mode of ex parte production of evidence* that constituted the "principal evil at which the Confrontation Clause was directed."[383]

Machine conveyances have become so probative and powerful that an algorithm like STRmix in the *Hillary* case can become the primary "accuser" in a criminal trial. While such software will surely help combat certain types of bias in forensic interpretation, it will create new types of bias a criminal defendant should have the right to explore.

If the Clause is concerned with unreliable, unconfronted testimony, then credibility-dependent claims that are likely unreliable and offered against the accused at trial should pose constitutional problems, particularly if the defendant does not have the opportunity to impeach the source. Several scholars have taken this view of the Clause, at least with respect to hearsay of human declarants,[384] and it was the view of the Supreme Court before 2004.[385] If unreliable,

---

382. Crawford v. Washington, 541 U.S. 36, 53 (2004).

383. People v. Lopez, 286 P.3d 469, 494 (Cal. 2012) (Liu, J., dissenting) (emphasis added) (quoting *Crawford*, 541 U.S. at 50).

384. *See, e.g.*, George Fisher, *The* Crawford *Debacle*, 113 MICH. L. REV. FIRST IMPRESSIONS 17, 19 (2014) (noting that the *Crawford* Court's fixation on testimony as a "solemn declaration" ignored another definition of testimony from the same source, as "[a] person who knows or sees any thing," and that nearly all hearsay should potentially implicate the Clause if there is no possibility for cross-examination); *cf.* Donald A. Dripps, *Controlling the Damage Done by* Crawford v. Washington*: Three Constructive Proposals*, 7 OHIO ST. J. CRIM. L. 521 (2010) (criticizing *Crawford*); Sklansky, *supra* note 312 (same). *But see* Friedman & Fisher, *supra* note 272, at 46 (arguing to retain the "testimonial" distinction).

385. *See* Ohio v. Roberts, 448 U.S. 56, 65-66 (1980), *abrogated by* Crawford v. Washington, 541 U.S. 36 (2004).

unconfronted testimony is the primary target of the Clause, then the accusatory output of proprietary software that has not been robustly tested would seem to be a problem potentially of constitutional magnitude.

Some scholars have suggested, along these lines, that the Clause be broadly construed, not only to guarantee courtroom testing of "witnesses," but also to "safeguard[] the ability of a defendant to probe and to fight back against the evidence offered against him."[386] I think that view is right, with a slight modification. The Clause does use the word "witnesses," and thus appears to address a particular kind of evidence—testimonial evidence. The Clause presumably has nothing to say about, for example, the state's use of physical evidence, or of facts that are only relevant to the extent that another fact might be inferred from them. The Due Process Clause might govern the state's failure to preserve or prove the integrity of physical evidence, but the Confrontation Clause presumably does not. In any event, there seems little reason to exempt unreliable machine sources from the definition of "witnesses" if reliability is the Clause's primary target.

Even under current doctrine, many machine conveyances would seem to implicate the Confrontation Clause. In 2004, in *Crawford v. Washington*, the Court dramatically shifted its approach and declared that the Clause applies only to so-called "testimonial hearsay."[387] If hearsay is testimonial, the right to courtroom testing is nearly categorical; generally, only if the defendant had a prior opportunity to cross-examine a now-unavailable declarant would testimonial hearsay from that declarant be admissible.[388] In turn, the question of what hearsay is "testimonial" has plagued lower courts since 2004. The *Crawford* Court adopted one of the definitions of "testimony" from Webster's dictionary: "[a] solemn declaration . . . made for the purpose of establishing or proving some fact."[389] A "casual remark to an acquaintance," however unreliable as evidence, would not be testimonial.[390] On the other hand, statements in response to police interrogation are testimonial,[391] unless the questioning ap-

386. Sklansky, *supra* note 312, at 71; *see also* Erin Murphy, *The Mismatch Between Twenty-First-Century Forensic Evidence and Our Antiquated Criminal Justice System*, 87 S. CAL. L. REV. 633, 657-58 (2014) (endorsing Sklansky's view).

387. *Crawford*, 541 U.S. at 51-53.

388. *Id.* at 59.

389. *Id.* at 51.

390. *Id.*

391. *See id.* at 68.

pears primarily intended to resolve an ongoing emergency,[392] because they resemble the old ex parte affidavit practice. Presumably, volunteered accusations, where the declarant is aware of the potential prosecutorial consequences, are also squarely testimonial.[393] Affidavits of forensic analysts, where the analyst certifies the reliability of the results of a laboratory process, are also generally testimonial,[394] although the Court appears close to revisiting that rule.[395]

Under *Crawford* and its progeny, machines seem capable of producing testimonial evidence, given the fitting analogy to ex parte affidavits. The primary sticking points are the Court's perpetual focus on hearsay, which by definition refers only to the out-of-court statements of people, and its assumption that only a "solemn declaration or affirmation made for the purpose of establishing or proving some fact"[396] can be testimonial. The focus on hearsay is, of course, understandable: the Framers were concerned primarily with human accusers, although bloodhound evidence presents an interesting point of comparison.[397] But even some of the current Justices appear to recognize that the application of the Clause to so-called "raw data generated by a machine" is an open question with a nonobvious answer,[398] much less the Clause's application to ma-

392. *See* Davis v. Washington, 547 U.S. 813, 822 (2006) (holding that statements are nontestimonial when "made in the course of police interrogation under circumstances objectively indicating that the primary purpose of the interrogation is to enable police assistance to meet an ongoing emergency").

393. *See, e.g.*, *id.* at 822 n.1.

394. *See* Melendez-Diaz v. Massachusetts, 557 U.S. 305, 310-11 (2009).

395. *See, e.g.*, Richard D. Friedman, *Rescued from the Grave and Then Covered with Mud: Justice Scalia and the Unfinished Restoration of the Confrontation Right*, 101 MINN. L. REV. HEADNOTES 39, 45, 49-50 (2016) (noting that several Justices seek to overturn *Melendez-Diaz* and disagree with some of *Crawford*'s central premises).

396. *Crawford*, 541 U.S. at 51 (quoting 2 NOAH WEBSTER, AN AMERICAN DICTIONARY OF THE ENGLISH LANGUAGE (1828)).

397. Lower courts generally do not view canines as witnesses. *See* Sites, *supra* note 16, at 63-64. The decisions of these courts generally began with the premise that the dog's credibility was not at issue. *See id.* If one instead began with the premise that a nonperson's credibility were implicated by an action or utterance, the confrontation question would be squarely presented, and it might be that dogs should also be "witnesses" under the Clause. For an exploration of the history of forensic dog tracking evidence as a means of supplanting human testimony, see Binyamin Blum, *The Hounds of Empire: Dog Tracking in Britain & Its Colonies, 1888-1953*, 35 LAW & HIST. REV. (forthcoming 2017) (on file with author).

398. Bullcoming v. New Mexico, 564 U.S. 647, 674 (2011) (Sotomayor, J., concurring). To the extent cases like *Bullcoming* reward the state for reducing the obvious human involvement in forensic output by reducing the level of scrutiny, my approach would force more inquiry in-

chine experts or advanced AI witnesses. It is also true that a machine source does not make a "solemn declaration" for the "purpose" of establishing facts, if such language assumes thought, intent, and an understanding of the moral gravity of one's accusation. *Crawford* took this phrase from a dictionary definition of testimony. While I sympathize with the view that *Crawford*'s focus on solemnity might have been misguided and ignored broader definitions of "testimony" in the same dictionary entry,[399] litigants have understandable difficulty convincing courts that machine conveyances are testimonial under this definition. Lower courts routinely hear, and reject, arguments that machine conveyances are covered by *Crawford*, in the context of digital infrared spectrometers and gas chromatographs reporting drug levels in blood;[400] DNA typing results;[401] breath test results;[402] Google Earth location data and satellite images;[403] red light camera timestamp data;[404] and computer-generated "header" data.[405] Some of these courts simply conclude that the Clause applies only to hearsay of persons, and no further analysis is required. Others correctly reason that machines are not aware of the prosecutorial consequences of their actions.

Even assuming the importance of solemnity in defining what evidence is "testimonial," machine sources should not be given an absolute pass under the

---

to less obvious human inputs that are not themselves testimonial hearsay but that affect the credibility of the accusatory machine output.

399. *See* sources cited *supra* note 384.

400. *See, e.g.*, United States v. Washington, 498 F.3d 225, 229-32 (4th Cir. 2007); People v. Lopez, 286 P.3d 469, 477-78 (Cal. 2012).

401. People v. Steppe, 152 Cal. Rptr. 3d 827, 835-36 (Ct. App. 2013) (citing Williams v. Illinois, 132 S. Ct. 2221 (2012), and *Lopez* for the proposition that "raw data" of DNA typing results could be admitted, and explained by a "technical reviewer," without the live testimony of the original analyst, because the results themselves are not testimonial); People v. Richards, No. B232300, 2012 WL 5866479, at *7-8 (Cal. Ct. App. Nov. 20, 2012) (citing *Lopez* and *Washington* for the proposition that admission of machine-generated results of a DNA analysis without the testimony of the particular DNA analyst who conducted the testing did not violate the Confrontation Clause).

402. *See, e.g.*, People v. Dinardo, 801 N.W.2d 73, 78-79 (Mich. Ct. App. 2010) (discussing whether the Datamaster breath test "ticket" is testimonial evidence); Boutang v. State, 402 S.W.3d 782, 787-89 (Tex. App. 2013) (discussing whether the Intoxilyzer print-out is testimonial evidence).

403. *See, e.g.*, United States v. Lizarraga-Tirado, 789 F.3d 1107, 1109-10 (9th Cir. 2015).

404. *See, e.g.*, People v. Goldsmith, 326 P.3d 239, 249-51 (Cal. 2014).

405. United States v. Hamilton, 413 F.3d 1138, 1142 (10th Cir. 2005) (holding that computer-generated header data on pornographic images uploaded by the defendant to a newsgroup was not hearsay); United States v. Khorozian, 333 F.3d 498, 506 (3d Cir. 2003) (holding that fax-generated header data was not hearsay).

Clause. If the point of targeting solemnity is to capture what is particularly abusive about the state purposely relying on impressive but unconfronted allegations of crime as a substitute for testimony, then machine sources would seem to be squarely implicated. When a complex proprietary algorithm is wielded by the state to create testimonial substitutes for human testimony that implicate the black box dangers, in a way that allows humans to evade moral responsibility for the act of accusation, the fact that the algorithm does not itself understand how it is being used seems beside the point.

2. *Rediscovering the Right of Meaningful Impeachment*

While the word "witnesses" presumably limits the type of evidence covered by the Clause to evidence that is in some broad sense testimonial, there is little reason to narrowly construe "confront[ation]" as guaranteeing only the courtroom safeguards of the oath, physical confrontation, and cross-examination. Courtroom mechanisms are only one path to testing credibility, one that is entrenched in Anglo-American evidence law for a variety of historical reasons. As David Sklansky has put it, the Court's focus on cross-examination is likely a product of its "fixation on the divide between common-law systems and civil-law systems" rather than the Clause's true animating principles.[406]

The Supreme Court has stated that "confrontation" has a broader meaning, beyond its most literal sense of physical confrontation. In upholding a state practice of allowing child victims to testify outside the defendant's presence by one-way closed circuit television, the Court in *Maryland v. Craig* noted that the "central concern" of the Clause is not to ensure an absolute right to physical confrontation, but "to ensure the reliability of the evidence . . . by subjecting it to rigorous testing."[407] "The word 'confront,' after all, also means a clashing of forces or ideas, thus carrying with it the notion of adversariness."[408] While the drafters of the Sixth Amendment clearly contemplated courtroom safeguards as the "elements of confrontation," the Court made clear that face-to-face confrontation "is not the *sine qua non* of the confrontation right."[409] Instead, it is the right of the defense "to probe and expose [testimonial] infirmities."[410]

---

406. *See, e.g.*, Sklansky, *supra* note 312, at 71-73.

407. Maryland v. Craig, 497 U.S. 836, 845 (1990).

408. *Id.*

409. *Id.* at 847.

410. *Id.* (quoting Delaware v. Fensterer, 474 U.S. 15, 22 (1985). While this results-oriented view of the Clause arguably was rejected in *Crawford*, nothing in *Crawford*'s language—and nothing

Moreover, the Supreme Court seems to have implicitly recognized that the common-law right of confrontation contemplated a general right of meaningful impeachment, rightly focused on general credibility testing rather than on particular courtroom mechanisms. In *Jencks v. United States*[411] and *Gordon v. United States*,[412] the Court required the prosecution to disclose witnesses' prior statements—with no showing of materiality or favorability to the defense—so the defense itself could determine their "impeaching weight and significance,"[413] and to avoid burying "important facts bearing on the trustworthiness of crucial testimony."[414] While *Jencks* and *Gordon* do not invoke the Sixth Amendment or a constitutional right of confrontation, at least one Justice later commented on the cases' "constitutional overtones,"[415] grounded in the "common-law rights of confrontation."[416] The cases stood for the "basic *Jencks* principle of assuring the defendant a fair opportunity to make his defense."[417] Such a right of impeachment would seem to contemplate credibility testing in general, not simply courtroom safeguards.

But with the passage of the Jencks Act quickly on the heels of these decisions in 1957, the underlying reasoning of cases like *Jencks* was lost. The Jencks Act by its terms applies only to witnesses who testify in court. But the purpose of that restriction, like the Act's pronouncement that only "substantially verbatim" statements of the witness[418] need be disclosed, was to ensure witness safety before trial, to avoid fishing expeditions, and to protect work product of government investigators.[419] Even giving full force to these concerns, there would seem little reason not to extend the principles of *Jencks* to machine sources.

---

about the animating principles underlying the Clause—precludes a view that the oath, cross-examination, and physical confrontation might be insufficient to ensure rigorous adversarial testing of a source.

411. 353 U.S. 657 (1957).

412. 344 U.S. 414 (1953).

413. *Id.* at 421.

414. *Id.* at 423.

415. Palermo v. United States, 360 U.S. 343, 363 (1959) (Brennan, J., concurring).

416. *Id.* at 362.

417. *Id.* at 365.

418. *See, e.g.*, Jencks Act, 18 U.S.C. § 3500 (2012); *Palermo*, 360 U.S. at 350 (holding that an agent's summary of an interview was not a "statement" for Jencks purposes).

419. 18 U.S.C. § 3500(b); S. REP. NO. 85-981, at 3 (1957), *as reprinted in* 1957 U.S.C.C.A.N. 1861, 1863-64 (noting that the Act was intended to address timing of disclosure and nature of statements, not to "curb, or to limit" *Jencks* "insofar as due process is concerned").

A right to meaningful impeachment of a nonhuman source might require much more, or less, than courtroom testing. Case-specific cross-examination of the programmer responsible for designing a software package may be unnecessary to probe the machine's potential for falsehood by design, inarticulateness, or analytical error due to design malfeasance or mistake. Instead, the programmer could give live testimony before some type of scientific commission, and return to the commission every time the software is changed or updated. Such a commission might seem anathema to existing adversarial structures, but a similar proposal for "advisory tribunals" to assess conflicting expert testimony was made by Learned Hand over a century ago,[420] and several bipartisan commissions have weighed in on how human forensic expert testimony should be presented.[421]

On the other hand, meaningful impeachment of a machine in a given case might require access to source code[422] or, alternatively, written answers to interrogatories that are completed by humans but that question the machine as if it were on cross-examination, such as "what population frequency statistics are you using in calculation of your likelihood ratio?" or "what threshold do you use in deciding what to call a genetic marker versus "noise"?" Meaningful impeachment might also include, where feasible, the presence of a defense expert at the time of testing to discourage and unearth case-specific input errors.[423] And it might require, as in *Jencks* itself, disclosure of prior statements of machines even when the prosecutor might not consider them "exculpatory" and

420. Learned Hand, *Historical and Practical Considerations Regarding Expert Testimony*, 15 HARV. L. REV. 40, 58 (1901).

421. *See, e.g.*, *Legal Resource Committee*, NAT'L INST. STANDARDS & TECH. (Jan. 5, 2017), http://www.nist.gov/topics/forensic-science/legal-resource-committee [http://perma.cc/VEX4-9UC5] (offering guidance on presentation of forensic expert testimony); Nat'l Comm'n on Forensic Sci., *supra* note 289; PCAST Report, *supra* note 149.

422. *Cf.* People v. Chubbs, No. B258569, 2015 WL 139069, at *4 (Cal. Ct. App. Jan. 9, 2015) (noting that the trial court had invoked the Confrontation Clause in ordering disclosure of source code to facilitate cross-examination of programmer); Order on Procedural History and Case Status in Advance of May 25, 2016 Hearing, United States v. Michaud, No. 3:15-CR-05351RJB, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016) (noting due process right to examine source code of government's Network Investigative Technique (NIT) used to hack defendant's computer).

423. *See also* Sklansky, *supra* note 312, at 74 (suggesting that confrontation in forensic science cases might require better "regulatory oversight of forensic labs, and facilitation of information-pooling by defense attorneys" (citing Erin Murphy, *The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence*, 95 CALIF. L. REV. 721, 777, 788-91 (2007))).

"material," thus removing them from the scope of disclosure as a matter of due process under *Brady v. Maryland*.[424]

Some might argue that the admission of machine evidence, a fast-changing field to be sure, should not turn on slow-moving constitutional litigation based on shaky doctrine. Hard-and-fast rules requiring, for example, the live testimony of a programmer for certain types of software might prove both overly burdensome on the state and unnecessary to meaningful impeachment. Perhaps, as a matter of strategy, reformers should focus their efforts on a workable, nonconstitutional impeachment standard for machine sources. But to immunize accusatory machine output from the Clause's reach entirely seems to be the wrong answer, at least as a theoretical, if not strategic, matter. *Daubert* and *Frye* are not constitutional requirements, and a state tomorrow could choose to admit relevant and authenticated machine conveyances with no credibility testing whatsoever.

In other contexts, the Sixth Amendment has a standard-based application that seems to work well without hard and fast rules that unduly curtail judicial discretion or burden parties. For example, the denial of certain lines of cross-examination is generally a matter within the sound discretion of the trial judge, but can rise to the level of a Sixth Amendment violation. Thus, a defendant who is prohibited "from engaging in otherwise appropriate cross-examination designed to show a prototypical form of bias on the part of the witness," critical to the jury's credibility determination, is denied his constitutional right of confrontation.[425] A similar standard might find a constitutional violation where the defendant is curtailed from testing a key aspect of the credibility of a critical machine source.

CONCLUSION

This Article has argued that certain machine evidence implicates the credibility of a machine source, that the black box dangers potentially plaguing machine sources trigger the need for credibility testing beyond what is contemplated by existing law, and that accusatory machine conveyances can be "witnesses against" a defendant under the Confrontation Clause. It has also offered a glimpse of the sorts of evidentiary and constitutional rules that might eventually govern machine sources of information. While we may never fully resolve the agency paradox underlying modern science, one does not have to

424. 373 U.S. 83 (1963).

425. Delaware v. Van Arsdall, 475 U.S. 673, 680 (1986).

believe that machines are entities capable of independent "thought" to understand the need to test their credibility or cabin the state's ability to hide behind their algorithmic accusations without robust credibility testing.

Exploring "machine testimony" reminds us that the law of *human* testimony has relied too heavily on a courtroom model of credibility testing and confrontation. Sometimes, the right to meaningfully impeach humans requires more than simply cross-examination. The Jencks Act, for example, does not apply to human hearsay accusers, even though access to the prior statements of hearsay declarants to impeach them through inconsistency, even if not on cross-examination, might be critical to the defense.[426] Federal Rule of Evidence 703 should perhaps require more scrutiny of assertions relied upon by human experts.[427] Front-end protocols, like the ones governing eyewitness identifications in some states, should be considered for other types of human testimony as well, such as on-scene witness statements to police officers. And jury instructions and corroboration rules should perhaps be considered for other types of human testimony.[428] Perhaps the sacred dichotomy between testimonial and physical evidence should itself be revisited; indeed, the Innocence Project has suggested treating eyewitness testimony as akin to trace evidence, the "result" of a process, just like courts have attempted to do with machine reports.[429] Meaningful impeachment of an eyewitness might move beyond cross-examination and toward access to experts. While human brains are not equivalent to a computer's black box,[430] cognitive psychologists have much to share that could avoid leaving juries with misimpressions about the probative value of human testimony.

---

426. *See, e.g.*, Watkins v. United States, 846 A.2d 293, 300 (D.C. 2004) (sympathizing with the argument that the Jencks Act should apply to hearsay declarants, but declining to exercise its supervisory power to fill the gap).

427. *See supra* text accompanying note 344.

428. *See, e.g.*, Sandra Guerra Thompson, *Beyond a Reasonable Doubt? Reconsidering Uncorroborated Eyewitness Identification Testimony*, 41 U.C. DAVIS L. REV. 1487, 1523-24 (2008) (arguing for a sufficiency rule requiring corroboration of eyewitness identification testimony). I do not mean to advocate jury instructions for their own sake; for many forms of human testimony, the jury's own life experience will offer sufficient context to accurately assess the testimony's probative value. But lawmakers should consider, more often and with more empirical grounding than they currently do, which types of testimony, outside accomplice and confession evidence, jurors might routinely over- or undervalue.

429. *See* Brief for The Innocence Project as Amicus Curiae Supporting Respondent at 30-33, State v. Henderson, No. 62,218 (N.J. Sept. 27, 2010) (2010 WL 11250988).

430. Robert Epstein, *The Empty Brain*, AEON (May 18, 2016), http://aeon.co/essays/your-brain-does-not-process-information-and-it-is-not-a-computer [http://perma.cc/VUS4-ZBDW].

The message of this Article is hopeful. While the Anglo-American system of proof is imperfect, to say the least, its strength is in its flexibility, which "creates space for experimentation with new approaches and also reduces the pressure for radical surgery on the existing system."[431] Creating new rules for machine sources, and adapting existing rules to accommodate machine sources, will not radically change our system of proof. Instead, recognizing machine conveyances as credibility-dependent will bring this critical area of conceptual and doctrinal confusion into line with the values underlying existing testimonial safeguards for human witnesses. If we do that, there is every reason to believe evidence law can "weather the coming tempests in proof technology."[432]

431. DAMAŠKA, *supra* note 8, at 151.

432. *Id.*