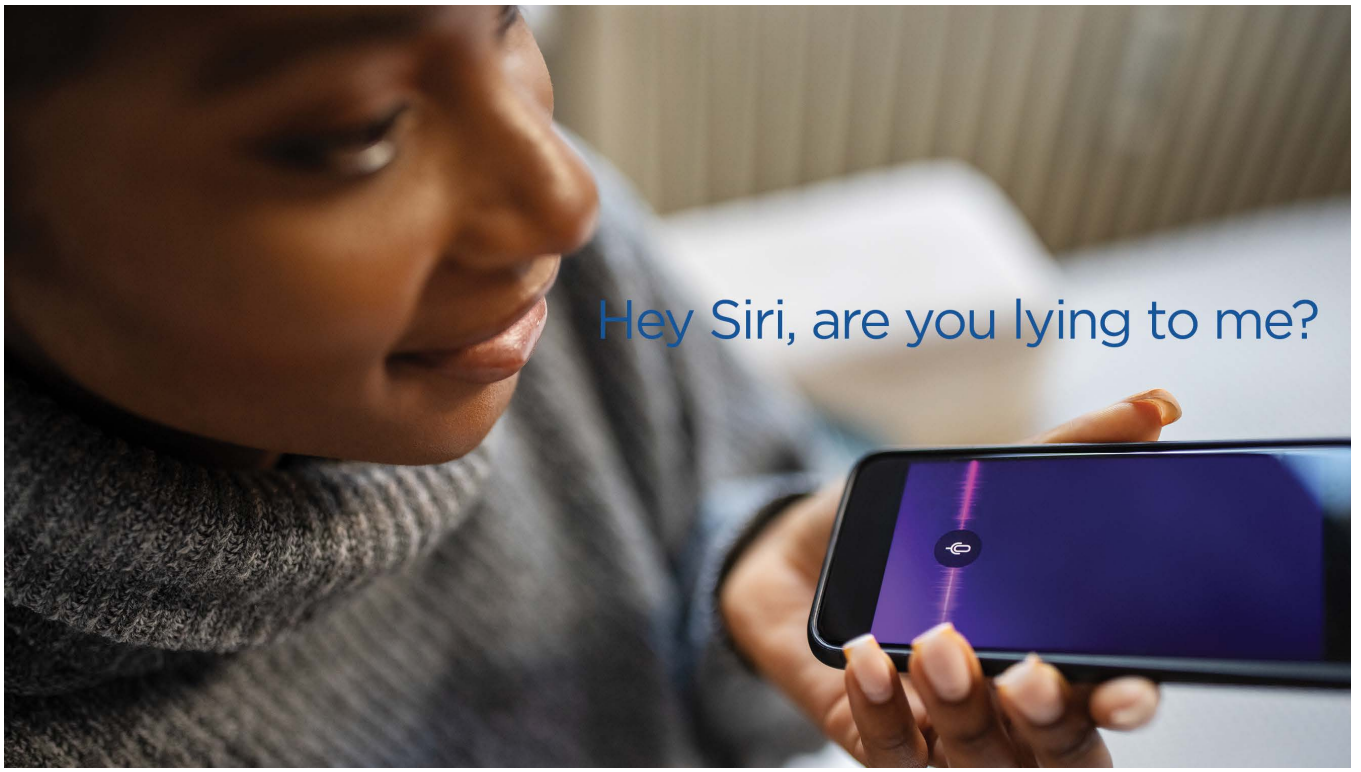
How Do You Cross-Examine Siri If You Think She's Lying?

By John M. McNichols, *Litigation News* Associate Editor



In March 1957, an officer stopped Preston Quick for driving 40 in a 30 mile per hour zone. To blame? A lead foot, but also a newly invented electric timer for clocking driving speeds. At trial, Quick challenged the admissibility of the timer's readout, arguing that it constituted hearsay because it was an out-of-court assertion offered for its truth. The St. Louis Court of Appeals rejected Quick's argument, explaining that under such logic, nearly every form of instrument-based evidence would be inadmissible—even the sounds of a stethoscope in a doctor's ear. The idea that Quick might have the right to probe how the timer arrived at its ultimate conclusion—or to cross-examine someone other than the arresting officer who testified about its operation—did not factor into the court's analysis at all.

In the decades since, most courts have followed suit, routinely admitting "machine testimony" that would undeniably be hearsay if originating from a human declarant. In doing so, courts have cited the perceived "objectivity" of such evidence over fallible human testimony. Meanwhile, the Federal Rules of Evidence define "hearsay" to encompass only statements by "a person." But the advent of artificial intelligence (AI) has called into question whether the traditional approach should still apply. The complexity of today's devices has long surpassed that of the timer Quick encountered, and as machines come ever closer to mimicking human thought, the need to challenge and "cross-examine" the evidence they provide may have arrived.

What Is AI?

Although there is no singular definition of AI, most technology writers use the term to describe the algorithmic coding that enables computers to analyze data and engage in autonomous decision-making to achieve pre-programmed objectives. AI is now a part of our daily lives, powering Apple's voice-operated personal assistant "Siri," self-driving cars, and—less interestingly, except perhaps to lawyers—document review software that can distinguish relevant e-discovery from irrelevant chaff. A computer's ability to undertake such tasks is often the result of "machine learning," the process of recognizing patterns in data to make assessments and predictions without human direction.

Unsurprisingly, AI has also found its way into the courtroom. There is no shortage of software designed to create forensic evidence, from blood-alcohol concentrations to the presence a particular person's DNA at a crime scene. In many instances, the software's report or "conclusion" is not a binary "yes"or"no"—or, as in Quick's case, a finite number—but rather is an expression of probability, more closely resembling a human opinion than a mathematical calculation.

What Are the Legal Issues Inherent in AI-Derived Evidence?

Hearsay is hardly the only potentially applicable objection to AI-derived evidence. As Professor Andrea Roth observes, when software functions as a "black box" shielding the algorithmic process connecting the underlying facts to the ultimate conclusion, it may be appropriate to challenge its reliability as expert testimony under Federal Rule of Evidence 703. This view, of course, likens the role of AI to that of a human expert, drawing on a body of esoteric knowledge to distill hard-to-grasp information into a form comprehensible to a lay jury.

Criminal defense attorneys have also invoked the Confrontation Clause to oppose software-derived evidence, again likening the software to a witness whom the accused should be permitted to confront through cross-examination. These challenges are more likely to be successful where the software was created specifically for courtroom use—such as with DNA analysis—and thus is undeniably "testimonial" under the U.S. Supreme Court's Crawford jurisprudence. Given the practical impossibility of cross-examining a computer program, however, counsel have had to be creative in proposing means to exercise the accused's confrontation right. Demands have included pretrial disclosure of the software's underlying source code and testimony of the software's designer.

Critics have noted that notwithstanding the supposed "objectivity" of machine-derived evidence, a computer program is only as fair and equitable as it is designed to be, and thus, any form of software can be biased depending on its underlying algorithms. Facial recognition technology, for example, is frequently subject to higher rates of misidentification of female and minority subjects, likely because of skewed sample sets in its underlying programming. Although awareness of this issue has prompted several municipalities to ban facial recognition technology for police use, one can expect that where it is still employed, criminal defendants will challenge the admissibility of technology-derived identifications on grounds of both reliability and its potential disparate impact on particular demographics.

What Is Next for AI-Derived Evidence?

Without doubt, the diversity and complexity of technological evidence available to juries today dwarfs that in existence at Preston Quick's trial in the 1950s. An outright ban on technology-derived evidence, therefore, would have the effect of needlessly depriving factfinders of relevant information—the very concern raised in Quick. In many cases, existing evidentiary rules and trial techniques are still adequate to test the reliability and credibility of machine evidence. As machines continue to take on new analytical capabilities independent of their users and designers, however, some new safeguards may be appropriate.

Some posit that pre-trial access to software's underlying source code would be sufficient to allow the party against whom it is introduced to scrutinize the logic and reasoning of its algorithms and, presumably, to expose any errors or biases in the advancing party's evidentiary conclusions. But skeptics contend that this is wholly unnecessary, noting that software can be rigorously tested simply by directing the software to analyze a set of control data. The same skeptics also note that source code frequently contains proprietary and commercially-sensitive components, and that requiring its disclosure will likely discourage companies from offering it for use in litigation.

Other scholars have contended that a heightened standard of admissibility—i.e., one that exceeds the prevailing *Daubert* standard for expert testimony—may be appropriate for certain forms of software-derived evidence. Cross-examination remains the primary means to challenge unreliable scientific or technical evidence, and thus, a more rigorous threshold test should apply where a litigant is, as a practical matter, unable to cross-examine the source of the evidence once it is admitted. As a supplemental screening tool, courts could demand, for example, evidence external to the software that corroborates its conclusions, akin to the new standard for the admission of hearsay under the residual exception of Federal Rule of Evidence 807. Until such time as machines can themselves be cross-examined, such a requirement may be courts' best option to ensure both consistency and transparency in AI-based evidence. LN

Today's devices are complex—as they come ever closer to mimicking human thought, the need to challenge and "cross-examine" their evidence may have arrived.

RESOURCES

- John M. McNichols, "Keeping One's Public Face Private," *Litigation News*, 46:3 (2021).
- *City of Webster Groves v. Quick*, 323 S.W.2d 386 (Mo. Ct. App. 1959).
- *United States v. Williams*, 382 F. Supp. 3d 928 (N.D. Cal. Apr. 29, 2019).
- *Pennsylvania v. Foley*, 38 A.3d 882 (Pa. Super. Ct. 2012).
- Katherine Kwong, "The Algorithm Says You Did It: The Use of Black Box Algorithms to Analyze Complex DNA Evidence," 31 *Harv. J.L. & Tech.* 275 (2017).
- Andrea Roth, "Machine Testimony," 126 *Yale L.J.* 1972 (2017)
- Paula Reed Ward, "Legal Question: How Do You Cross-Examine a Computer?," *Pittsburgh Post-Gazette* (Aug. 29, 2016).
- Lael Henterly, "The Troubling Trial of Emanuel Fair," *Seattle Weekly* (Jan. 11, 2017).
- 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).
- Christian Chessman, Note, "A 'Source' of Error: Computer Code, Criminal Defendants, and the Constitution," 105 *Calif. L. Rev.* 179 (2017).
- Brian Sites, "Rise of the Machines: Machine-Generated Data and the Confrontation Clause," 16 *Colum. Sci. & Tech. L. Rev.* 36 (2014).
- Michael L. Rich, "Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment," 164 *U. Pa. L. Rev.* 871 (2016).
- Pamela S. Katz, "Expert Robot: Using Artificial Intelligence to Assist Judges in Admitting Scientific Expert Testimony," 24 *Alb. L.J. Sci. & Tech.* 1 (2014).