Machine-Created Evidence: A Myth of Objectivity?

Bias can easily be an inherent part in machine-created evidence, experts say.

By Rhys Dipshan, Law Technology News

May 2, 2017

With the proliferation of digital data, courts have moved to regulate how certain electronic information should be handled and when it can be used in courts. And though not always permitted as evidence, the veracity of electronic information often goes unquestioned by judges and jurors alike. Some legal professionals, however, view this as naïve and shortsighted.

Machine-created evidence is already influencing many trial processes and outcomes. In a panel at New York University School of Law's "Algorithms and Explanations" event, Andrea Roth, assistant professor of law at the University of California at Berkeley Law School, noted that machine-generated proof is already supplied by a multitude of technology, from breath analyzers, polygraph tests, radar guns and red-light cameras to DNA interpretation software and even such common internet tools as Google Earth.

These types of evidence, she said, are supposed to be better received than testimony provided by human witnesses because of the unfortunate fact that the credibility of such witnesses can often be shaded by biases or prejudices. However, she added, machine-generated evidence is far from unequivocal.

As an example, Roth cited a famous homicide case in Potsdam, New York, involving local soccer coach Oral Nicholas Hillary, a prime suspect in the death of his ex-girlfriend's son. When investigators sent low traces of mixed DNA from the deceased boy's fingernails to a lab that analyzed the sample with a software called TrueAllele, the test results found no connection with Hillary.

But years later, at the behest of then-new Onondaga County District Attorney William Fitzpatrick, the DNA was analyzed by a new forensic software called STRmix. This time, the lab "determined [Hillary] was very likely to be a contributor" of the DNA found under the victim's fingernails, Roth said.

While STRmix's evidence was ultimately deemed impermissible in court and Hillary was acquitted, it is difficult to conclude one DNA test was more objective than the other. Though TrueAllele dismissed STRmix's results as being subjective and partially aided by human interpretation, whereas its analysis was fully done by machines, there is no easy way to prove that TrueAllele's analysis was wholly impartial.

Roth explained there are technical and operational limits to understanding how TrueAllele's DNA tests were conducted given that "TrueAllele has 170,000 lines of code," so one cannot easily hand over that information to an attorney.

"The problem is, you can't cross-examine a computer," she added, noting the laws of evidence that courts use are created for human evidence, not algorithmic or electronic evidence. While some bypass this discrepancy by arguing that a software or machine's programmer should answer for any decisions its tools make, Roth noted that "does not make sense" given the autonomous and complex ways machines can learn and decide.

Machine Bias's Catch-22

Though machine-generated evidence is relied on as a way of circumventing biases in humans, there can be cases where it instead creates and propagates biases in those deciding sentencing terms and reprimands. In the NYU panel, Paul Rifelj, a former judge for the Milwaukee County Circuit Court in Wisconsin, singled out the use of the sentencing risk assessment tool COMPAS, which uses algorithms to measure former prisoners' recidivism and reoffense risks, as potentially infringing on a judge's impartiality.

"Judges read what risk assessment COMPAS reports before the bell has rung" and any hearing gets underway, he said, arguing that the judges are therefore influenced "by that label, be it low, medium or high" risk that these reports provide.

While Rifelj added that COMPAS put out a disclaimer which notes that the software is "not to be used in determining whether or not somebody goes to prison or for how long," he does not "believe for one second that when a judge sees that someone is likely to commit a violent crime over the next five years, he or she is able to ignore that."

What's more troubling, Rifelj noted, is that some COMPAS assessments are not entirely calculated by machines. "Between 8 and 15 percent of the time, almost one in seven reports can be changed" by a COMPAS evaluator's subjective evaluation.

Yet even if all the assessments were automated, Rifelj still believes there is the very real problem of not being able to know how the COMPAS algorithms assess risk in the first place.

The right to access such information was recently litigated in multiple state courts in Wisconsin, relating to the conviction of Eric Loomis, a resident found guilty in connection with a drive-by shooting. After his sentencing, Loomis filed a motion for postconviction relief, arguing that the court's use of the COMPAS assessment—one of the many factors the court considered—violated his due process rights. When Loomis demanded to know how COMPAS assessed his risk, the court denied him access to the data because it deemed the information proprietary and a trade

secret.

Loomis's legal challenge eventually made it to the Wisconsin Supreme Court, which last July affirmed the lower court's ruling. In its decision, the court stated, "Ultimately, we conclude that if used properly, observing the limitations and cautions set forth herein, a circuit court's consideration of a COMPAS risk assessment at sentencing does not violate a defendant's right to due process."

Rifelj, however, worried about "the idea of sentencing and caging human beings with these algorithms which are secret," adding that it goes against the law's culture of transparency.

"We don't allow ex parte communication, and we demand that defendants can control their witnesses," he said. "So why not demand the same level of trust from software?"

Contact Rhys Dipshan at rdipshan@alm.com. On Twitter: @R_Dipshan.
