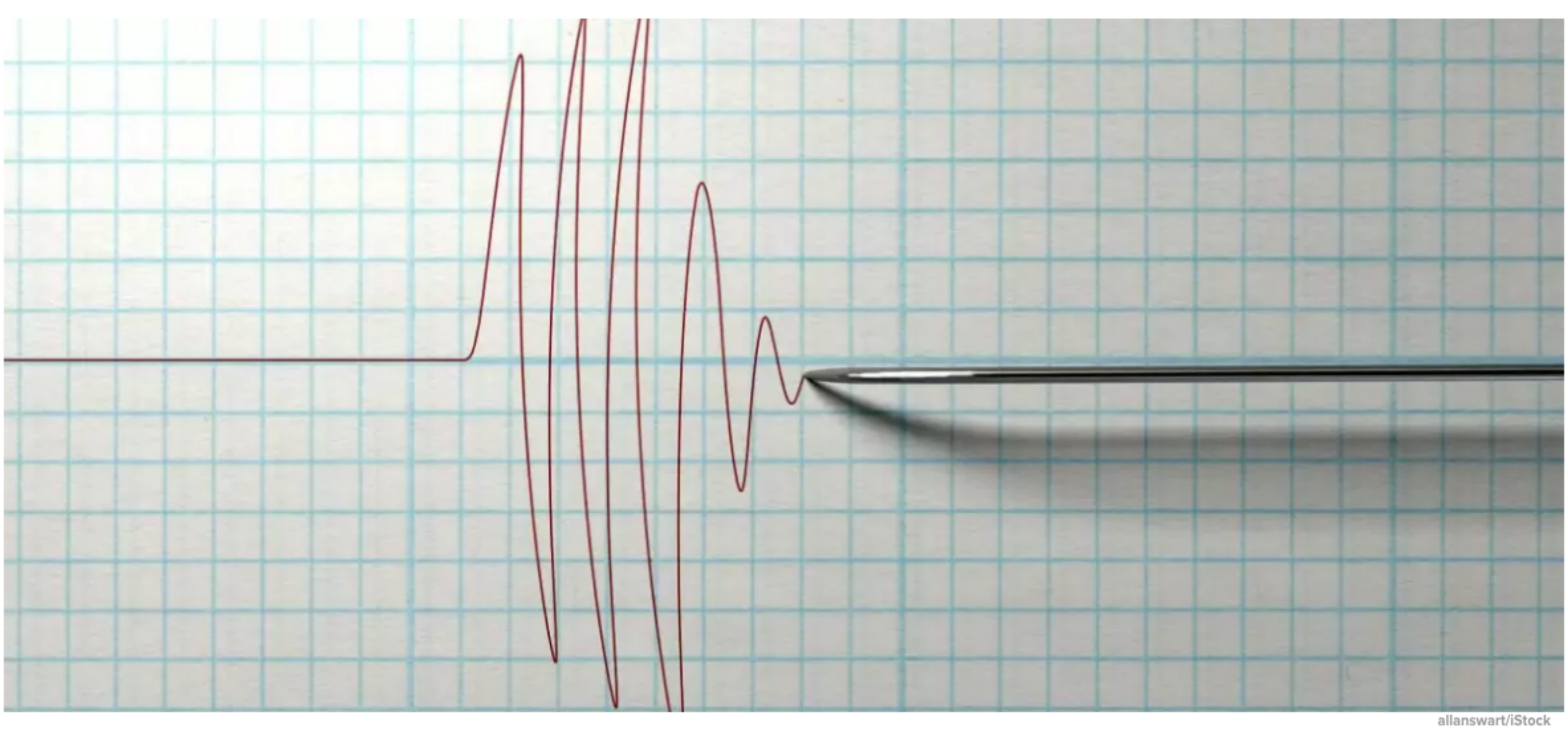
THE WEEK

FEATURE

The false promise of the lie detector

Amit Katwala



allanswart/iStock

October 5, 2019

Excerpted from an article that originally appeared in The Guardian. *Used with permission.*

We learn to lie as children, between the ages of 2 and 5. By adulthood, we are prolific. We lie to our employers, to our partners, and most of all, one study has found, to our mothers. The average person hears up to 200 lies a day, according to research by Jerry Jellison, a psychologist at the University of Southern California. The majority of the lies we tell are "white," the inconsequential niceties — "I love your dress!" — that grease the wheels of human interaction. But most people tell one or two "big" lies a day, says Richard Wiseman, a psychologist at the University of Hertfordshire. We lie to promote ourselves, to protect ourselves, and to hurt or avoid hurting others.

The mystery is how we keep getting away with it. Our bodies expose us in every way. Hearts race, sweat drips, and micro-expressions leak from small muscles in the face. We stutter, stall, and make Freudian slips. "No mortal can keep a secret," wrote the psychoanalyst in 1905. "If his lips are silent, he chatters with his fingertips. Betrayal oozes out of him at every pore."

Even so, we are hopeless at spotting deception. On average, across 206 scientific studies, people can separate truth from lies just 54 percent of the time — only marginally better than tossing a coin. Some people stiffen and freeze when put on the spot; others become more animated. Liars can spin yarns packed with color and detail, and truth-tellers can seem vague and evasive.

Humans have been trying to overcome this problem for millennia. The search for a perfect lie detector has involved torture, trials by ordeal, and, in ancient India, an encounter with a donkey in a dark room. In 1730, the English writer Daniel Defoe suggested taking the pulse of suspected pickpockets. "Guilt carries fear always about with it," he wrote. "There is a tremor in the blood of a thief." More recently, lie detection has largely been equated with the juddering styluses of the polygraph machine. But none of these methods has yielded a reliable way to separate fiction from fact.

That could change. In the past couple of decades, the rise of cheap computing power, brain-scanning technologies, and artificial intelligence has given birth to what many claim is a powerful new generation of lie-detection tools. Startups, racing to commercialize these developments, want us to believe that a virtually infallible lie detector is just around the corner.

Their inventions are being snapped up by police forces, state agencies, and nations desperate to secure themselves against foreign threats. They are also being used by employers, insurance companies, and welfare officers. "We've seen an increase in interest from both the private sector and within government," said Todd Mickelsen, CEO of Converus, which makes a lie detector based on eye movements and subtle changes in pupil size.

Converus' technology, EyeDetect, has been used by FedEx in Panama and Uber in Mexico to screen out drivers with criminal histories, and by the credit-ratings agency Experian, which tests its staff in Colombia to make sure they aren't manipulating the company's database to secure loans for family members. In the U.K., police are carrying out a pilot scheme that uses EyeDetect to measure the rehabilitation of sex offenders. Other EyeDetect customers include the government of Afghanistan, McDonald's, and dozens of local police departments in the United States. Soon, large-scale lie-detection programs could be coming to the borders of the U.S. and the European Union, where they would flag potentially deceptive travelers for further questioning.

★★

But as tools such as EyeDetect infiltrate more and more areas of public and private life, there are urgent questions to be answered about their scientific validity and ethical use. Nothing provides a clearer warning about the threats of the new generation of lie detectors than the history of the polygraph, the world's most widely used deception test.

John Larson, the inventor of the polygraph, came to hate his creation. In 1921, Larson was a 29-year-old rookie police officer working the downtown beat in Berkeley, California. But he had also studied physiology and criminology, and when not on patrol he was in a lab at the University of California, developing ways to bring science to bear in the fight against crime.

In the spring of 1921, Larson built an ugly device that took continuous measurements of blood pressure and breathing rate, and scratched the results onto a rolling paper cylinder. He then devised an interview-based exam that compared a subject's physiological response to questions relating to a crime with the subject's response to control questions such as "Is your name Jane Doe?" As a proof of concept, he used the test to solve a theft at a women's dormitory.

Larson refined his invention over several years with the help of an enterprising young man named Leonarde Keeler, who envisioned applications for the polygraph well beyond law enforcement. After the Wall Street crash of 1929, Keeler offered a version of the machine concealed inside an elegant walnut box to large organizations so they could screen employees suspected of theft.

Not long after, the U.S. government became the world's largest user of the exam. During the Red Scare of the 1950s, thousands of federal employees were subjected to polygraphs designed to root out communists. The U.S. Army, which set up its first polygraph school in 1951, still trains examiners for all the intelligence agencies at the National Center for Credibility Assessment at Fort Jackson in South Carolina.

Companies also embraced the technology. Through much of the last century, about a quarter of U.S. corporations ran polygraph exams on employees to test for issues including histories of drug use and theft. By the 1980s, there were up to 10,000 trained polygraph examiners in the United States, conducting 2 million tests a year.

The only problem was that the polygraph did not work. In 2003, the U.S. National Academy of Sciences published a damning report that found evidence on the polygraph's accuracy across 57 studies was "far from satisfactory." History is littered with examples of known criminals who evaded detection by cheating the test. Aldrich Ames, a KGB double agent, passed two polygraphs while working for the CIA in the late 1980s and early '90s. With a little training, it is relatively easy to beat the machine. Floyd "Buzz" Fay, who was falsely convicted of murder in 1979 after a failed polygraph exam, became an expert on the test during his two and a half years in prison and started coaching other inmates on how to defeat it.

The polygraph remained popular, though — not because it was effective, but because people thought it was. "The people who developed the polygraph machine knew that the real power of it was in convincing people that it works," said Dr. Andy Balmer, a sociologist at the University of Manchester who wrote a book called *Lie Detection and the Law*.

The threat of being outed by the machine was enough to coerce some people into confessions. One examiner in Cincinnati in 1975 left the interrogation room and reportedly watched, bemused, through a two-way mirror as the accused tore 6 feet of paper charts off the machine and ate them. You didn't even have to have the right machine: In the 1980s, police officers in Detroit extracted confessions by placing a suspect's hand on a photocopier that spat out sheets of paper with the phrase "He's Lying!" pre-printed on them.

Other people were pushed to admit to crimes they did not commit after the machine wrongly labeled them as lying. The polygraph became a form of psychological torture that wrung false confessions from the vulnerable. Many of these people were then charged, prosecuted, and sent to jail — whether by unscrupulous police and prosecutors or by those who wrongly believed in the polygraph's power.

★★

Some people believe an accurate lie detector would have allowed border agents to stop the 9/11 hijackers. As a result, the front lines for much of the new government-funded lie-detection technology have been the borders of the U.S. and Europe. In 2014, travelers flying into Bucharest were interrogated by a virtual border agent called Avatar, an onscreen figure in a white shirt with blue eyes that introduced itself as "the future of passport control." In addition to an e-passport scanner and a fingerprint reader, the Avatar unit has a microphone, an infra-red eye-tracking camera, and an Xbox Kinect sensor to measure body movement. It is one of the first "multi-modal" lie detectors — one that incorporates a number of different sources of evidence — since the polygraph.

But the "secret sauce," according to David Mackstaller, who is taking the technology in Avatar to market via a company called Discern Science, is in the software, which uses an algorithm to combine all of these types of data. The machine aims to send a verdict to a human border guard, within 45 seconds, who can either wave travelers through or pull them aside for additional screening. Mackstaller said he is in talks with governments — he wouldn't say which ones — about installing Avatar permanently after further tests at Nogales in Arizona, on the U.S.-Mexico border, and with federal employees at Reagan Airport near Washington, D.C. Discern Science claims accuracy rates in its preliminary studies, including the one in Bucharest, have been between 83 percent and 85 percent.

Mackstaller said Avatar's results will improve as its algorithm learns. He also expects it to perform better in the real world, because the penalties for getting caught are much higher, so liars are under more stress. But research shows that the opposite may be true: Lab studies tend to overestimate real-world success.

The accuracy rates of 80 percent to 90 percent claimed by the likes of EyeDetect and Avatar sound impressive, but applied at the scale of a border crossing, these tools would lead to thousands of innocent people being wrongly flagged for every genuine threat they identified. It might also mean that two out of every 10 terrorists would easily slip through.

History suggests that such shortcomings will not stop these new tools from being used. After all, the polygraph has been widely debunked, but an estimated 2.5 million polygraph exams are still conducted in the U.S. every year. It is a $2.5 billion industry. In the U.K., the polygraph has been used on sex offenders since 2014, and in January 2019, the government announced plans to use it on domestic abusers on parole. The test "cannot be killed by science because it was not born of science," writes the historian Ken Alder in his book *The Lie Detectors*.

New technologies may be harder than the polygraph for unscrupulous examiners to deliberately manipulate, but that does not mean they will be fair. AI-powered lie detectors prey on the tendency of both individuals and governments to put faith in science's supposedly all-seeing eye. And lie detectors often get aimed at society's most vulnerable: women in the 1920s, suspected dissidents and homosexuals in the '60s, welfare claimants in the 2000s, asylum seekers and migrants today.

In an era of fake news and falsehoods, it can be tempting to look for certainty in science. But lie detectors tend to surface at "pressure-cooker points" in politics, when governments lower their requirements for scientific rigor, said Balmer. In this environment, dubious new techniques could "slip neatly into the role the polygraph once played," Alder predicts.

One day, improvements in artificial intelligence could find a reliable pattern for deception by scouring multiple sources of evidence, or more detailed scanning technologies could discover an unambiguous sign lurking in the brain. In the real world, however, practiced falsehoods — the stories we tell ourselves about ourselves, the lies that form the core of our identity — complicate matters. "We have this tremendous capacity to believe our own lies," Dan Ariely, a renowned behavioral psychologist at Duke University, said. "And once we believe our own lies, of course we don't provide any signal of wrongdoing."