“Lordy, I hope there are tapes,” said an exasperated James Comey in his testimony before the Senate Intelligence Committee on June 8. Comey's desire reflects a familiar one for individuals accused of lying when the stakes are high. The former FBI director wished for tapes because, in our society, audio and video recordings serve as a final arbiter of truth. He said, she said always loses to what the tape shows.

Today, when people see a video of a politician taking a bribe, a soldier perpetrating a war crime, or a celebrity starring in a sex tape, viewers can safely assume that the depicted events have actually occurred, provided, of course, that the video is of a certain quality and not obviously edited.

But that world of truth—where seeing is believing—is about to be upended by artificial intelligence technologies.

We have grown comfortable with a future in which analytics, big data, and machine learning help us to monitor reality and discern the truth. Far less attention has been paid to how these technologies can also help us to lie. Audio and video forgery capabilities are making astounding progress, thanks to a boost from AI. In the future, realistic-looking and -sounding fakes will constantly confront people. Awash in audio, video, images, and documents, many real but some fake, people will struggle to know whom and what to trust.

Lyrebird, a deep learning tech startup based in Montreal, is developing technology that allows anyone to produce surprisingly realistic-sounding speech with the voice of any individual. Lyrebird’s demo generates speech, including varied intonation, in the voices of Donald Trump, Barack Obama, and Hillary Clinton. For now, the impersonations are impressive, but also possess a fuzzy, robotic quality that allows even an untrained ear to easily recognize the voice as computer-generated. Still, the technology is making rapid progress. Creative software giant Adobe is working on similar technology, announcing its goal of producing “Photoshop for audio.”

Researchers at Stanford and elsewhere have developed astonishing capabilities in video forgery. Using only an off-the-shelf webcam, their AI-based software allows an individual to realistically change the facial expression and speech-related mouth movements of an individual on YouTube video. Watch as one researcher edits a video of George W. Bush to insert new facial and speech expression, all in real time.

Other AI research groups have demonstrated the ability to run image recognition capabilities in reverse, allowing the generation of synthetic images based on text description alone. Jeff Clune, one of the researchers leading this work, told The Verge that “people send me real images and I start to wonder if they look fake. And when they send me fake images I assume they're real because the quality is so good.”

Combined, the trajectory of cheap, high-quality media forgeries is worrying. At the current pace of progress, it may be as little as two or three years before realistic audio forgeries are good enough to fool the untrained ear, and only five or 10 years before forgeries can fool at least some types of forensic analysis. When tools for producing fake video perform at higher quality than today’s CGI and are simultaneously available to untrained amateurs, these forgeries might comprise a large part of the information ecosystem. The growth in this technology will transform the meaning of evidence and truth in domains across journalism, government communications, testimony in criminal justice, and, of course, national security.

The Russian intelligence service employs thousands of full-time workers who author fake news articles, social media posts, and comments on mainstream websites. These agents in turn control millions of botnet social media accounts that tweet about politics in order to shape national discourse. A study by the Computational Propaganda Research Project at the Oxford Internet Institute found that half of all Twitter accounts regularly commenting about politics in Russia were bots. And these operations don’t stop at the Russian border: In the US, Russian social media bots have already demonstrated an ability to drive mainstream media coverage of fake news and even influence American stock prices.

What happens when those agents and botnets are also armed with the ability to automatically generate and share not merely fake tweets of fake news but also fake HD video and audio? The technology industry and governments should not stand idly by to find out. The threats from the rise of this technology are multifaceted. So, too, must be the solutions.

Some will be technological in nature. Just as there are (admittedly imperfect) technological solutions that attempt to prevent image software like Photoshop from being used to counterfeit money, there may be technological solutions that can mitigate the worst impacts of AI-enabled forgery. Blockchain, the same technology used to secure cryptocurrencies such as Bitcoin, offers one possibility: It provides cryptographically secured evidence for the ordering of bitcoin transactions so that no one can spend the same cryptocurrency twice. It may be possible to design cameras and microphones that use blockchain technology to create an unimpeachable record of the date of creation of video recordings. While this would not prevent later editing or forged counterevidence, it would at least allow cryptographically secured evidence to show that a given file existed at a certain date, which could allow experts to infer that later versions may have been edited.

Other solutions will be regulatory and procedural. Police officers and prosecutors may have to develop standards of evidence for proving the chain of custody of a particular camera or microphone. An anonymously emailed video file may ultimately become as irrelevant as anonymously emailed witness testimony is today. And all manner of institutions may come to have a new appreciation for conversations held face to face around a table when phone calls and video chats may not only be digitally intercepted but also digitally impersonated.

Since the late 1800s, with the invention of the photograph and phonograph, society has had access to technology that can, with some important caveats, provide an answer in disputes about the truth. President Richard Nixon said he had no knowledge of the Watergate burglary coverup. The tapes proved that he lied. Unless government and business leaders seriously face this challenge, we will have to live in a society where there is no ultimate arbiter of truth. Perhaps in 10 years James Comey’s prayer will be answered and tapes will emerge of his conversations with Donald Trump. At that point, however, citizens and historians alike will have to wonder whether the tapes are real or yet another case of AI-enabled forgery.

Greg Allen (@Gregory_C_Allen) is an adjunct fellow at the Center for a New American Security. WIRED Opinion publishes pieces written by outside contributors and represents a wide range of viewpoints. Read more opinions here.