Deepfakes Are Coming. We Can No Longer Believe What We See.

It will soon be as easy to produce convincing fake video as it is to lie. We need to be prepared.

By Regina Rini
Dr. Rini teaches philosophy at York University in Toronto.

June 10, 2019

[1] On June 1, 2019, the Daily Beast published a story exposing the creator of a now infamous fake video that appeared to show House Speaker Nancy Pelosi drunkenly slurring her words. The video was created by taking a genuine clip, slowing it down, and then adjusting the pitch of her voice to disguise the manipulation.

[2] Judging by social media comments, many people initially fell for the fake, believing that Ms. Pelosi really was drunk while speaking to the media. (If that seems an absurd thing to believe, remember Pizzagate; people are happy to believe absurd things about politicians they don’t like.)

[3] The video was made by a private citizen named Shawn Brooks, who seems to have been a freelance political operative producing a wealth of pro-Trump web content. (Mr. Brooks denies creating the video, though according to the Daily Beast, Facebook confirmed he was the first to upload it.) Some commenters quickly suggested that the Daily Beast was wrong to expose Mr. Brooks. After all, they argued, he’s only one person, not a Russian secret agent or a powerful public relations firm; and it feels like “punching down” for a major news organization to turn the spotlight on one rogue amateur. Seth Mandel, an editor at the Washington Examiner, asked, “Isn’t this like the third Daily Beast doxxing for the hell of it?”

[4] It’s a legitimate worry, but it misses an important point. There is good reason for journalists to expose the creators of fake web content, and it’s not just the glee of watching provocateurs squirm. We live in a time when knowing the origin of an internet video is just as important as knowing what it shows.

[5] Digital technology is making it much easier to fabricate convincing fakes. The video that Mr. Brooks created is pretty simple; you could probably do it yourself after watching a few YouTube clips about video editing. But more complicated fabrications, sometimes called “deepfakes,” use algorithmic techniques to depict people doing things they’ve never done — not just slowing them down or changing the pitch of their voice, but making them appear to say things that they’ve never said at all. A recent research article suggested a technique to generate full-body animations, which could effectively make digital action figures of any famous person.
So far, this technology doesn’t seem to have been used in American politics, though it may have played some role in a political crisis in Gabon earlier this year. But it’s clear that current arguments about fake news are only a taste of what will happen when sounds and images, not just words, are open to manipulation by anyone with a decent computer.

Combine this point with an insight from epistemology — the branch of philosophy dealing with knowledge — and you’ll see why the Daily Beast was right to expose the creator of the fake video of Ms. Pelosi. Contemporary philosophers rank different types of evidence according to their reliability: How much confidence, they ask, can we reasonably have in a belief when it is supported by such-and-such information?

We ordinarily tend to think that perception — the evidence of your eyes and ears — provides pretty strong justification. If you see something with your own eyes, you should probably believe it. By comparison, the claims that other people make — which philosophers call “testimony” — provide some justification, but usually not quite as much as perception. Sometimes, of course, your senses can deceive you, but that’s less likely than other people deceiving you.

Until recently, video evidence functioned more or less like perception. Most of the time, you could trust that a camera captured roughly what you would have seen with your own eyes. So if you trust your own perception, you have nearly as much reason to trust the video. We all know that Hollywood studios, with enormous amounts of time and money, can use CGI to depict almost anything, but what are the odds that a random internet video came from Hollywood?

Now, with the emergence of deepfake technology, the ability to produce convincing fake video will be almost as widespread as the ability to lie. And once that happens, we ought to think of images as more like testimony than perception. In other words, you should only trust a recording if you would trust the word of the person producing it.

Which means that it does matter where the fake Nancy Pelosi video, and others like it, come from. This time we knew the video was fake because we had access to the original. But with future deepfakes, there won’t be any original to compare them to. To know whether a disputed video is real, we’ll need to know who made it.

It’s good for journalists to start getting in the habit of tracking down creators of mysterious web content. And it’s good for the rest of us to start expecting as much from the media. When deepfakes fully arrive, we’ll be glad we’ve prepared. For now, even if it’s not ideal to have amateur political operatives exposed to the ire of the internet, it’s better than carrying on as if we can still trust our lying videos.

Regina Rini (@rinireg) teaches philosophy at York University in Toronto, where she holds the Canada Research Chair in Philosophy of Moral and Social Cognition.