online spotlight

Mary Ellen Bates
Bates Information Services

Say What? 'Deepfakes' Are Deeply Concerning

As any good industry observer will tell you, the best way to predict the future is to watch the players known for pushing the envelope. When it comes to online content, the industry that has blazed the trail is, well, pornography. Adult websites drove the early development of real-time credit card processing, streaming video, live chat (between performers and customers), and pay-per-click ads. So when I heard about "deepfakes," a new artificial intelligence (AI) project showing up in the pornosphere, I paid attention.

Combine "deep learning" and "fake videos" and you get deepfakes—AI-based software that can superimpose someone's face onto an existing image or video. Celebrities' faces have been inserted into pornographic videos; the resulting fake videos are said to be difficult to identify as false. Were this development limited to smut, we info pros could simply feel grateful that our research doesn't usually veer into the prurient. But, as with pay-per-click ads and real-time credit card payments, what the porn industry initially capitalizes on, the rest of the online world eventually adopts as well. You can already create your own fake videos using Fakeapp, a free mobile app.

For an alarming vision of the possible impact of deepfakes on the information landscape, check out a fake video of Barack Obama warning about the danger of fake videos (vox.com/2018/4/18/17252410/jordan-peele-obama-deepfake-buzzfeed). Warning: "Obama" uses some uncharacteristically bad language in this video. While this video was created with actor Jordan Peele voicing Obama, new text-to-speech technology such as CereProc (cereproc.com) can create a "clone" of an individual's voice that sounds remarkably similar to the original. As far back as 2011, film critic Roger Ebert used CereProc to synthesize his voice when he lost his ability to speak after cancer surgery.

Perhaps the most alarming development, given the deep pockets of the developer, is Google Duplex, an AI voice chatbot technology that can generate natural-sounding speech, complete with "ums" and "ahs," capable of conducting scheduling tasks. Listen to a couple of phone calls in which Google Duplex interacts with real humans to set up appointments (ai.googleblog.com/2018/05/duplex-ai-system-for-natural-conversation.html), and shudder.

What is particularly worrisome about these developments is that we humans are hardwired to trust our eyes and ears. Add our confirmation bias into the mix, and it becomes obvious that we are facing a serious challenge. Imagine a political candidate producing a video that purports to show the opponent saying something controversial or an advocacy group publishing a video appearing to show misbehavior of a public official. Claims of "fake news" are already so prevalent, the victim of a faked video may not be able to establish credibility by claiming that the evidence has been falsified. Teaching our clients and patrons not to trust their senses is a tough sell, and there is a fine line between advocating a healthy skepticism about something on the web that just doesn't seem right and sounding like a tin-foil-hat-wearing paranoid.

While I do not see any easy solutions, one approach we info pros can take is to encourage confidence in the organizations that are dedicated to providing verified and sourced information. We can provide our clients information from, or access to, value-added information resources that contain trusted sources and content that has not been altered or modified. We can find creative ways to promote information literacy and information hygiene, teaching our clients to discern reliable news from dodgy sources and encouraging a bit of doubt when a news item sounds too good to be true.

Taking a bigger perspective on combatting the threat of information manipulation, info pros can play a role in advocating for tools that can rebuild our trust in photos and audio and video recordings—and here is where blockchain technology may play a role. While blockchain has been associated in the public mind with cryptocurrencies and shady dealings, it could be the best defense against manipulated audio or video files. Blockcerts (blockcerts.org), for example, is a free app that takes digital records such as a university graduation record and issues a blockchain-based official record that can be shared with a third party. Anyone who receives a copy of the record can verify its validity by comparing it to the original version stored in the blockchain.

Imagine if news organizations used a similar technique to sign and seal news footage. Granted, this still requires trust that the person creating the image or the audio or video recording did not alter the data file, but it reduces the possibility of a post-publication manipulated version of the file being accepted as true by enabling anyone to compare a copy to the blockchain-based original. Protecting the integrity of a digital image or recording may soon become as important a role for info pros as preserving print content.

__Mary Ellen Bates__ (mbates@BatesInfo.com, Reluctant-Entrepreneur.com) doesn't even use Photoshop on her pictures.

Comments? Email the editor-in-chief (marydee@xmission.com).