FALL 2019 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery, and cybersecurity needs. For this E-Newsletter, we provide an overview of deepfake technology and the impact on the legal industry. We also explore the regulatory climate and new developments.

Deepfake Dangers Highlight the Need for Authentication

Scarlett Johansson, Natalie Portman, and Gal Gadot have more in common than earning millions in superhero blockbusters. They're all victims of deepfake, nonconsensual pornography. Johansson recognizes that she can't stop anyone from using video manipulation technology from stealing her image. "The fact is that trying to protect yourself from the Internet and its depravity is basically a lost cause…" said the understandably irked movie star (https://gizmodo.com/scarlett-johansson-on-deepfakes-the-internet-is-a-vast-1831399330). The misappropriation of a celebrity's image is just one of the dangers of deepfakes, and the range of deepfake dangers is increasing almost as rapidly as the technology can be improved. But are deepfakes really that dangerous?

Not Just the Rich and Famous

The more images with which a deepfake app can be trained, the better the deepfake quality that can be produced. Hence, with the near infinite number of celebrity images available, the potential quantity of training material for a deepfake application is more than enough to create a high-quality product. But what about an average person just posting selfies on social media? The sad reality is that as deepfake technology improves, higher quality deepfakes can be created with a smaller set of training data, down to a single image. For example, there is only one Mona Lisa, and that was all a Samsung lab located in Moscow needed to create a "living" Mona Lisa deepfake (https://youtu.be/P2uZF-5F1wI).

Seeing is Believing

Most people understand the content of a movie on the big screen is fiction. But when we're on social media, and our trusted friends, family members, and coworkers post a video they believe

is true, we're more inclined to lend it credence. If that video is of a real politician, but the content is fake, it can erode not just our trust in political leaders, but our trust in governments, news providers, social media platforms, and each other. Experts understand this and are working to combat malicious deepfakes, but they warn we're rapidly approaching a level of deepfake expertise that's confounding experts, not just the general public. Dr. Hany Farid, a leading researcher on deepfakes, has said that deepfake technology is improving dramatically every three to six months, making it harder to tell an authentic image or video from a deepfake (https://www.theguardian.com/technology/2018/nov/12/deep-fakes-fake-news-truth).

Dr. Farid and his team at the University of California at Berkeley are working on the problems of detecting deepfakes, but they aren't the only ones. No less than the US government's Defense Advanced Research Projects Agency, Facebook, and Google are all working with private companies including digital forensics firms, academic laboratories, and individuals to collaborate on technology to detect deepfakes (https://ai.facebook.com/blog/deepfake-detection-challenge/; https://ai.googleblog.com/2019/09/contributing-data-to-deepfake-detection.html; https://www.darpa.mil/program/semantic-forensics). How serious are these organizations about detecting deepfakes? Facebook alone is dedicating a total of ten million dollars to fund the effort and provide incentives for people to contribute to the detection technology, and hopefully, make the distribution of such available to companies that work in digital forensics. Google has already publicly released a database of known deepfakes for the benefit of detection research.

The Highest Stakes

Government elections are target-rich environments for deepfakes, and researchers are concerned that social media sites, news outlets, and other media dissemination sites are being flooded with deepfakes attempting to muddy political waters around the globe. The United States' national election in the year 2020 is already marked as a high stakes race for both deepfake creators and detection researchers. The deepfake problem could easily play out two ways: (1) deepfake videos of candidates doing or saying things that influence voters, or, (2) candidates being authentically "caught" but claiming that the video or audio is a deepfake https://www.npr.org/2019/09/02/754415386/what-you-need-to-know-about-fake-video-audio-and-the-2020-election). Either way, voter trust may be eroded with negative impacts on the election and the country. If you think that's far-fetched, a Belgian political party created a deepfake using US President Trump in 2018 to sway voter opinion. The video includes a spoken line revealing that the video is fake, however, that disclaimer is omitted from the subtitled text of the video (https://www.economist.com/leaders/2018/05/24/a-faked-video-of-donald-trump-points-to-a-worrying-future). The video demonstrates a few key "tells," such as blurring around the edge of the face and asynchronous timing between the mouth movements and the speech, that in a year since the posting of the video, are now correctable by the latest deepfake software.

Digital Mountain and other digital forensics experts are working hard to adopt and improve the latest technology to authenticate source material from potential deepfakes. With the ability of deepfake programs to create deepfakes from fewer and fewer images, it won't be long until deepfake revenge videos become digital evidence in the courtroom. Lawyers and those hired to present expert testimony will need to know how the technology works and how to tell the authenticated source material from the deepfakes.

Movie-goers and technology enthusiasts alike praise advances in video manipulation that allow cinematographers to bring back our beloved but deceased actors, like Carrie Fischer as Princess Leia. We can suspend our disbelief for the duration of the film and simply enjoy the magic of

Hollywood. But when we see an outrageous video of a world leader going viral, or we hear that a friend has been identified in an ugly video posted by a former partner, we need to recall the dangers of deepfake technology and engage our disbelief, because our insistence on the truth, the whole truth, and nothing but the truth, is vital for us all.

Please direct questions and inquiries about cybersecurity, computer forensics and electronic discovery to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

OPENTEXT ENFUSE 2019
Las Vegas, NV: November 11-14, 2019

TODAY'S GENERAL COUNSEL, "THE EXCHANGE" EDISCOVERY
San Francisco, CA: November 19, 2019

INFOSECURITY NORTH AMERICA AND ISACA
New York, NY: November 20-21, 2019

GEORGETOWN LAW'S 2019 ADVANCED EDISCOVERY INSTITUTE
Washington, DC: November 21-22, 2019

TODAY'S GENERAL COUNSEL, "THE EXCHANGE" EDISCOVERY
Los Angeles, CA: December 11, 2019

Click here to see more upcoming events and links

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.

4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: