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 Legislation: Deeply Complex

When you're the US state known for technology innovation, rapidly developing legislative responses to those innovations seems to be imperative to good governance. California, while not the first state to pass legislation attempting to address the problems associated with deepfake technology, recently passed and signed into law legislation that affords candidates for public office an opportunity to seek damages and injunctive relief against someone who maliciously distributes an injurious, unacknowledged deepfake sixty days prior to an election (https://www.mercurynews.com/2019/10/04/california-has-a-new-deepfakes-law-in-time-for-2020-election/). The law doesn't apply until January 1, 2023, making it moot for the 2020 national campaign, but still, as a warning to would-be deepfake creators intent on injecting disinformation into the political process, they can't say California hasn't telegraphed its intentions. The new law does, however, raise two important questions – what about now and what about the rest of us? Is there no current legal remedy to help victims of deepfakes? And how are non-political figures protected from deepfake harm?

Can't Wish It Away

Technology, in and of itself, is neutral – it's neither inherently good, nor inherently evil. The problem arises when technology is weaponized. Deepfake technology is no exception. For example, the same technology that has been utilized to create nonconsensual pornography is also being harnessed to give back to Motor Neuron Disease (also known as ALS and Lou Gehrig's Disease) patients their voices and allow them to create authentic speech (https://www.projectrevoice.org/). Deepfake technology is also being employed to create interactive, educational exhibits such as *Dali Lives!* where patrons at the Dali Museum in Florida can learn from the artist himself about his life, his inspiration, and his works from a series of deepfake Dalis (https://thedali.org/press-room/dali-lives-museum-brings-artists-back-to-life-with-ai/). It's easy to see how outlawing the technology simply to prevent its misuse would also rob us of its benefits.

A Full Range of Protection

Some legal scholars argue that new deepfake-centric laws aren't necessary to combat the misuse of deepfake technology because between criminal law and tort law, we already have all the legal force needed to bring down the gavel on those who create malicious fictitious videos. The Electronic Frontier Foundation's David Greene wrote in 2018 about existing criminal and civil laws that can be used to fight deepfake abuse, including laws covering extortion, harassment, False Light, defamation, Intentional Infliction of Emotional Distress, right of publicity, and in certain cases, copyright infringement (https://www.eff.org/deeplinks/20-18/02/we-dont-need-new-laws-faked-videos-we-already-have-them). Additionally, forty-six states, the District of Columbia, and the US territory Guam currently have statutes enacted that can be applied to nonconsensual pornography. So, yes, there is a case to be made for a sufficiency of existing legislation.

On the federal level in the US, there is a provision of the Communications Decency Act (CDA), which is Title V of the Telecommunications Act of 1996, that has been receiving a lot of attention recently in light of the viral spread of deepfakes on social media platforms. Section 230 of the CDA provides some immunity to social media platforms when it comes to removing content from their sites. There's been wide latitude given under Section 230 in that social media platforms are merely "hosts" for the content posted by users, and therefore, not responsible for policing the veracity of deepfakes posted and shared by users. That immunity for social media sites merely allowing deepfakes to passthrough from user to user on their sites is currently under scrutiny. While there are exceptions, the precedent for enforcing takedown actions against platforms has been largely unsuccessful apart from *Barnes v. Yahoo!, Inc. (Barnes v. Yahoo!, Inc., 570 F. 3d 1096 - Court of Appeals, 9th Circuit 2009*). In *Barnes*, the facts of the case state that a Yahoo! employee agreed to remove a series of false profiles of the plaintiff posted by a former boyfriend. When Yahoo! failed to remove the fake content, Barnes sued and the court agreed that while the CDA did provide protection for the profiles themselves, the promise of the Yahoo! employee to remove the posts created a contractual agreement between the parties which Yahoo! needed to fulfill. It's no wonder then that social media platforms have been very clear that they are not content editors, although recently various platforms have voluntarily begun to examine the issue (https://www.cnet.com/news/facebook-twitter-and-youtube-grapple-with-altered-videos-ahead-of-the-2020-election/).

Dr. Martin Luther King, Jr. is attributed to having said, "Even though morality cannot be legislated, behavior can be regulated," (https://www.usnews.com/news/blogs/press-past/2013/01/21/martin-luther-king-in-his-own-words). And just as the hammer can be used to build a house or break a window, and earbuds can be used to create privacy or decrease our awareness of what's happening around us, deepfake technology can spread lies, or give the power of speech to those who have lost theirs. Whether we have sufficient legal remedies to correct the malicious behavior of those who use the technology to harm, there's no doubt that we're only on the cusp of trying to legislate our way to an answer.

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: