FALL 2024 E-NEWSLETTER

At Digital Mountain, we assist our clients with their electronic discovery, digital forensics, cybersecurity, and data analytics needs. For this E-Newsletter, and Cybersecurity Awareness Month, we discuss how deepfakes create expensive problems for organizations, a review of deepfake technology, and the slow march toward deepfake legislation.

Deepfake Legislation: Zombies Move Faster

Talk about deepfake legislation can be overheard in the halls of nearly any state or federal government building. No wonder, too, as it's presidential election season and we're seeing deepfakes of candidates and celebrity endorsements going viral. With their ability to convincingly convey misleading and false information, deepfakes could undermine our republic's stability. But what about the other harmful ways in which deepfakes are being used? What legislation do we have to protect our kids, public figures, and our hard-earned savings from criminals with computers? In the face of a threat that's growing exponentially, does the law really need to move slower than a lumbering zombie? For this article, we'll look at what's happening on the deepfake legislation front and why it can be an uphill fight.

According to the public interest nonprofit advocacy group Public Citizen, as of September 30, 2024, 29 states have enacted legislation addressing intimate deepfakes "falsely depicting a real person engaging in…" well, you know (interactive legislation tracker). While this is a laudable start, many of these enacted laws only apply to minors being depicted in intimate deepfakes. Conversely, more than 60 pieces of legislation regarding deepfakes have failed. The Regulatory Transparency Project, a nonprofit arm of The Federalist Society, believes state laws addressing intimate deepfakes should be narrowly constructed because the topic is already covered by Section 230 of the Communications Decency Act (Regulatory Transparency Project article). State representatives like Matthew Bierlein of Michigan who see the value in state-level intimate deepfake laws, are hopeful that, "If we get this done, then maybe Ohio adopts this in their legislative session, maybe Indiana adopts something similar, or Illinois, and that can make enforcement easier," (Wired.com article).

California Governor Gavin Newsom signed three bills in September that address both sexually explicit deepfakes and watermarking AI-generated content with the goal to make AI-generated content safer and more transparent (SB 942, watermarking; SB 926, sexually explicit deepfakes; and, SB 981 (deepfake identity theft) were all passed. SB 926 defines unauthorized sexually

explicit deepfakes as a crime, and SB 981 provides a take-down provision allowing for victims to address unwanted deepfakes quickly. These bills are being heralded as wins for those targeted deepfakes, and as a step forward for AI-watermarking.

Federally, two bills addressing intimate deepfakes were introduced by two very disparate legislators. New York City representative Alexandra Ocasio-Cortez introduced the Defiance Act on March 7, 2024, which would allow for victims of intimate deepfakes to sue for civil damages and seek other protections. Not long after, Senator Ted Cruz of Texas introduced the Take It Down Act which not only includes mandated prison sentences for creators of intimate deepfakes, but also includes provisions for victims to demand that intimate deepfakes be removed from internet platforms. As of October 3, 2024, the Take It Down Act had cleared the Senate Commerce, Science and Transportation Committee, and the Defiance Act, in its Senate form has passed the Senate and was in committee in the House (congress.gov – bill search).

While attention to deepfakes that take aim at politicians are receiving worldwide attention, one bill was recently met with a legal challenge. California's AB 2839, signed into law by Governor Newsom on September 17, 2024, would "allow any political candidate, election official, the Secretary of State, and everyone who sees his AI-generated videos to sue him for damages and injunctive relief during an election period which runs 120 days before an election to 60 days after an election," (court order), has been temporarily struck down by Judge John Mendez of the US District Court in the Eastern District of California. The rapidity of the takedown is striking, as the legislation was signed on September 17, 2024, and the Preliminary Injunction granted on October 3, 2024. In the First and Fourteenth Amendment challenges to the bill, the Court agrees with the plaintiff, a deepfake creator of political parodies and satires who convincingly argued that "counter speech is a less restrictive alternative to prohibiting videos such as those posted by Plaintiff, no matter how offensive or inappropriate someone may find them," (ibid). This may not be the end of this fight, but for now, more political deepfakes are on the way in California.

Deepfake victims are not sitting back while their images are being manipulated for nefarious purposes and legislation lingers in limbo. Australian businessman Andrew Forrest has filed a lawsuit against Facebook parent, Meta Platforms, Inc. over the appearance of deepfake ads. The ads contain deepfake images and voices of Dr. Forrest that were used to help promote cryptocurrency scams. Meta tried to get the suit dismissed under Section 230(c)(1) of the Communications Decency Act. Dr. Forrest successfully argued:

> [t]hat Meta has "active involvement" in deciding what ads look like and who they are shown to and that its automated tools "supercharge Meta's ability to produce and drive the Scam Ads to vulnerable viewers," which has "been a substantial factor in the continuing production, dissemination, and success" of the challenged ads (Order).

Whether Dr. Forrest is ultimately able to hold the social media giant liable for appearance of deepfake ads on the platform or not, the trial will certainly spark debate about the how best to control the dissemination of these deceptions.

Clearly, the battle to prevent deepfake harm continues, even if it's waged at the pace of a pack of lumbering zombies. But with the rise in state-based legislative activity, the promise of more federal legislation being introduced in both the House and the Senate, and some high-profile lawsuits, it may not be an eternity before the law provides some redress for victims – be they politicians or regular people. Or at least people with pulses and brains.

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

UPCOMING INDUSTRY EVENTS

THE SEDONA CONFERENCE WORKING GROUP 11
MIDYEAR MEETING 2024
Atlanta, GA: October 29-30, 2024

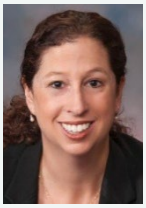
CISO-CIO FORUM
La Jolla, CA: October 30, 2024

MASTERS CONFERENCE NOVEMBER 2024
Atlanta, GA: November 12, 2024

GEORGETOWN LAW 21ST ANNUAL ADVANCED EDISCOVERY INSTITUTE
Washington, DC: November 14-15, 2024

OPENTEXT WORLD 2024
Las Vegas, NV: November 19-21, 2024

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: