Texas Public POLICY FOUNDATION

TESTIMONY BEFORE THE JOINT STUDY COMMITTEE ON EFFECTS OF MEDIA ON MINORS

BY **Zach Whiting,** Texas Public Policy Foundation
JANUARY 7, 2025

Dear Co-Chair Hughes, Co-Chair Patterson, and Committee Members,

My name is Zach Whiting, and I am a policy director and senior fellow at the Texas Public Policy Foundation. Thank you for holding this hearing and for the opportunity to testify. The Foundation is incredibly grateful for the tremendous work the Legislature and each committee member has done over the past few sessions to keep kids safe, particularly from the serious impacts and harms of certain forms of media.

My oral testimony will speak to broader policy considerations related to the specific charges of social media, AI, and mobile devices. This written testimony will provide an excerpt from our recently published AI research paper, highlighting the harms AI presents through deepfakes and sexual exploitation of minors (Whiting & Dunmoyer, 2024).

According to Somers (2020), "the term 'deepfake' was first coined in late 2017 by a Reddit user of the same name. This user created a space on the online news and aggregation site, where they shared pornographic videos that used open source face-swapping technology" ("What is a deepfake?" section). The term is a portmanteau: it is "an artificial [or 'fake'] image or video (a series of images) generated by a special kind of *machine learning* called 'deep' learning" (University of Virginia, n.d., para. 3).

Technologically, deepfakes are not new, but the ability to fabricate life-like audio, images, and sound more accurately, quickly, and cheaply has accelerated recently. Deepfake technologies can be used for fun and entertainment, like creating emotion-evoking photo filters, funny videos of dancing animals, and buzzworthy pictures of Pope Francis in a white puffer coat.

Journalist Simon Chandler (2020) bemoaned the concerns and "worst-case scenario[s]" being raised about deepfake technologies, and he instead argued that "much more realistically, deepfake technology will play an increasingly constructive role in recreating the past and in envisioning future possibilities" (para. 4). He went so far as to say that "deepfakes are your friend," and "the ability to generate realistic simulations using artificial intelligence will, on the whole, be only a positive for humanity" (para. 1). He provided several examples:

continued

- "Experienc[ing] things that no longer exist, or that have never existed."
- "Recreating long-dead artists in museums."
- "Transform[ing] Da Vinci's famed Mona Lisa into video, using deep learning to show the subject of the painting moving her eyes, head and mouth."
- "Creat[ing] 'lost' audio of the speech JFK was due to give in Dallas on November 22, 1963, the day he was assassinated."
- Generating AI-driven news presenters and news "reports personalised for each individual news viewer."
- "Editing video without the need for a reshoot"
- "Creat[ing] 'fake' brain MRI scans" and "by training algorithms on these medical images and on 10% real images, these algorithms became just as good at spotting tumours as an algorithm trained only on real images."
- Having David Beckham deliver "an anti-malaria message in nine languages." (Chandler, 2020, paras. 2–12)

However, nefarious actors are also weaponizing deepfake technology to confuse, intimidate, lie, coerce, and exploit. Previous sections discussed harmful threats in the realm of national security, cybersecurity, elections, and broader epistemological concerns—that is, how we know whether something is real or not. This section will consider some of the effects of deepfakes on individuals. The world is entering a future where posting a completely innocent picture or creating a voice memo supplies nefarious actors with all the ammunition they need. Victims of deepfakes—from celebrities to high schoolers to grieving parents to grandparents scammed out of their retirement savings—will probably take little solace in Chandler's admonition that deepfakes are our "friends."

For example, in 1993, James Bulger, a two-year-old boy from the U.K., was abducted, tortured, and killed by two ten-year-old boys. However, in July 2023, AI-generated clips brought James "back to life" to talk about his murder and blame his mother for not taking care of him when he was kidnapped at a grocery store. Many other so-called "trauma porn" videos run rampant on TikTok, YouTube, in Google search results, and elsewhere, generating millions of views (Lodge, 2024; Hassan, 2023).

Other nefarious actors use deepfakes and voice cloning to trick and defraud. For example, in Brooklyn, New York, couple Robin and Steve were awoken in the middle of the night by a phone call from Steve's parents, Mona and Bob. On the other end, Robin heard Mona screaming and pleading. Then the voice of an assailant, "a relaxed male voice—possibly Southern," came on the phone and said, "I've got a gun to your mom's head, and I'm gonna blow her brains out" unless Robin and Steve sent $500 via Venmo using a pizza emoji (Bethea, 2024, para. 3). The assailant called back and demanded another $250. Robin and Steve paid.

In another instance, a St. Louis mother received a call from her daughter saying she got into a fender bender. A male voice came on the phone and demanded a $2,000 wire transfer from a local Walmart, or he would kidnap the daughter. The mother descried the experience to a local NBC News affiliate:

> Toward the end, they put my daughter back on the phone. It basically said, "Mom, do what they say." She said her daughter's voice sounded so real that she never thought it was a scam. (Krall, 2024, paras. 8–9)

In another instance, Jennifer DeStefano, a Scottsdale, Arizona, mother was called by what she was convinced was her 15-year-old daughter, who profusely apologized for "messing up," followed by a man's voice demanding a $1 million ransom payment for the safe return of her daughter. Jennifer later said, "A mother knows her child. … You can hear your child cry across the building, and you know it's yours" (Karimi, 2023, para. 12). Jennifer was convinced.

However, Mona and Bob were never held at gunpoint. They did not even make the call—their number was spoofed, and their voices were deepfaked. The St. Louis daughter was never in a fender bender or at risk being kidnapped. And Jennifer's daughter was never being kidnapped. She was away training for a ski race. Instead, all were victims of deepfake scams. CBS News recently reported that generating these types of deepfakes is not difficult, time consuming, or costly:

> After a quick Google search, [news reporter Masha] Saeidi found an AI-powered website and paid $5 to use its voice cloning service. Next, she needed a 30-second audio clip of the voice she wanted to replicate. CBS New York's investigative executive producer loaned his voice, but Saeidi also could've pulled it from his social media. With just those few simple steps, she was able to make his AI-generated voice say whatever she typed. The whole process, from the time it took to create the account to generating the cloned voice, took about two to four minutes. The startup behind the website told Saeidi the technology can be used to narrate a book or give a voice to those without one. (Saeidi, 2024, "How easy is it to clone someone's voice?" section)

These scams are raking in lots of money, as "data from the Federal Trade Commission shows in the past four years, scams involving business imposters have been on the rise. Last year, more than $752 million was lost" (para. 3). Furthermore, as noted above, "Hong Kong police announced that a finance worker had been tricked into paying out twenty-five million dollars after taking part in a video conference with who he thought were members of his firm's senior staff. (They were not.)" (Bethea, 2024, para. 13). Indeed, this is a very sophisticated deepfake scam and shows the lengths that cybercriminals will go for a major payoff.

Another nefarious use of deepfakes is to sexually harass, manipulate, coerce, and exploit others. It is sobering (although perhaps not surprising) that 98% of all deepfake videos online are pornographic and that 99% of the individuals targeted in deepfake pornography are female (Security Hero, 2023). Tenbarge (2023) reported that "according to Sensity, an Amsterdam-based company that detects and monitors AI-developed synthetic media … 96% of deepfakes are sexually explicit and feature women who didn't consent to the creation of the content" (para. 5).

In early 2024, AI-generated sexualized images of singer Taylor Swift appeared online and were "viewed tens of millions of times" across social media platforms before being removed (Kelly, 2024, para. 2). As Steele (2023) noted, "deepfake porn is far from victimless. It has been wielded against women as a weapon of blackmail, an attempt to destroy their careers, and as a form of sexual assault" (para. 4).

The generation and dissemination of child sexual abuse material (CSAM) is the most reprehensible application of deepfake technologies. Unfortunately, the sad reality is that criminals seem to be a step ahead, and rapid advancements in artificial intelligence and emerging technologies only make the challenges of taking down child predators that much harder. With this technology, harmful and even irreparable abuse can be committed for free and in minutes. This means child predators can easily weaponize the technology to create child sexual abuse materials. For example, Verma (2023) reports that

> a rise in cheap and easy-to-use AI tools that can "undress" people in photographs—analyzing what their naked bodies would look like and imposing it into an image—or seamlessly swap a face into a pornographic video. On the top 10 websites that host AI-generated porn photos, fake nudes have ballooned by more than 290 percent since 2018, according to Genevieve Oh, an industry analyst. (para. 4)

However, celebrities are not the only targets for sexualized deepfakes. For example, "over 30 girls between the ages of 12 and 14 in a Spanish town were recently subject to deepfake porn images of them spreading through social media" (Steele, 2023, para. 4). In the United States,

> boys in several states have used widely available "nudification" apps to pervert real, identifiable photos of their clothed female classmates, shown attending events like school proms, into graphic, convincing-looking images of the girls with exposed A.I.-generated breasts and genitalia. In some cases, boys shared the faked images in the school lunchroom, on the school bus or through group chats on platforms like Snapchat and Instagram, according to school and police reports. (Singer, 2024, para. 8)

A 14-year-old New Jersey girl, Francesca Mani, was among 30 victims of sexually explicit deepfakes created and shared by male classmates (Tenbarge, 2024). In Texas, 15-year-old Elliston Berry and at least six of her friends were the victims of sexualized deepfake photos. In the case of Berry, a real family photo of her standing on a cruise ship was used to create a deepfake nudifying her. The photos were spread via anonymous Snapchat accounts and text messages (Jargon, 2024). Senator Ted Cruz and other colleagues have introduced a series of bills to fight back against this.

To see how widespread the problem is, consider the following statistics and trends over the last decade. According to a 2019 story,

> there are at least 14,678 deepfake videos—and counting—on the internet, according to a recent tally by a startup that builds technology to spot this kind of AI-manipulated content. And nearly all of them are porn. The number of deepfake videos is 84% higher than it was last December when Amsterdam-based Deeptrace found 7,964 deepfake videos during its first online count. (Metz, 2019, paras. 2–3)

According to another report, by 2023, just four years later, the total number of deepfake videos online was 95,820, up 550% from 2019. Pornography made up 98% of them (Security Hero, 2023, "Key Findings" section). Steele (2023) reported that "the ten leading dedicated deepfake porn sites had monthly traffic of 34,836,914 this year. And the deepfake videos and images go far beyond the bounds of deepfake porn sites; 70% of the top porn sites also host deepfake porn" (para. 2). Furthermore, Tenbarge (2023) reported that

> an NBC News review of two of the largest websites that host sexually explicit deepfake videos found that they were easily accessible through Google and that creators on the websites also used the online chat platform Discord to advertise videos for sale and the creation of custom videos. (para. 4)

Specially, Tenbarge found that

> the spike [in Google search traffic] also coincided with an uptick in the number of videos uploaded to MrDeepFakes, one of the most prominent websites in the world of deepfake porn. The website hosts thousands of sexually explicit deepfake videos that are free to view. It gets 17 million visitors

> a month, according to the web analytics firm SimilarWeb. A Google search for "deepfake porn" returned MrDeepFakes as the first result. (para. 8)

The statistics for online child exploitation are even more sobering. According to the FBI Internet Crime Center Report, in 2020, cybercrimes "against children increased by 144% compared to 2019—that's 8 children per day facing online exploitation" (Surfshark, n.d., "Cybercrime against children year over year" section). Of particular relevance to this section, in an article appropriately titled "Generative AI CSAM is CSAM," the National Center for Missing & Exploited Children (NCMEC) (2024) said it received 4,700 reports of generative AI child porn and sexually exploitative images in 2023.

Even before generative AI, the internet's supply of child sexual abuse imagery was rapidly expanding. AI technologies only accelerate it. According to the Internet Watch Foundation (2022), "255,588 [website] reports were confirmed as containing child sexual abuse imagery, having links to the imagery, or advertising it" (p. 3). Furthermore, more than 125 million CSAM-related posts were removed by major online platforms in 2021, many of them deepfaked (Whiting, 2023b).

Finally, in addition to the federal efforts by Sen. Cruz and others, state lawmakers are considering several ways to combat abusive deepfakes. The National Conference of State Legislatures [NCSL] (2024b) noted that "at least 40 states have pending legislation in the 2024 legislative session. At least 50 bills have been enacted" (para. 6). In 2023, Texas enacted HB 2700 (2023), which adds AI and deepfake-generated sexually explicit materials targeting children to the list of prohibitions in three sections of Penal Code. In a June 2024 interim hearing, prosecutors testified that while grateful for the law, they are hamstrung by the requirement for the materials to depict an "actual" child rather than any depiction of what is, indeed, child pornography (The Texas Senate, 2024). One solution for Texas lawmakers to consider is to change the "actual" standard to "indistinguishable." As the NCMEC noted, such a change would punish "users of the technology to create this material [who] have used the argument that, 'At least I didn't hurt a real child' and 'It's not actually a child'" (National Center for Missing & Exploited Children, 2024, para. 3).

Thank you, again, for the opportunity to testify today. The Foundation stands at the ready to assist you and your staff on this and any other issues.

Sincerely,

Zach Whiting

The Honorable Zach Whiting
Policy Director and Senior Fellow
Better Tech for Tomorrow
Texas Public Policy Foundation
zwhiting@texaspolicy.com

ABOUT THE AUTHOR

The Honorable Zach Whiting is Policy Director and Senior Fellow for Better Tech for Tomorrow at the Texas Public Policy Foundation.

Prior to joining the Foundation, he served as a state senator in his native state of Iowa. He served as Assistant Majority Leader, chair of the Labor and Business Relations Committee, and vice chair of the Administrative Rules Review Committee. Prior to the senate, Zach worked as a Legislative Assistant and Policy Advisor to a member of Congress. He graduated summa cum laude with a B.A. in political science from Stetson University and earned a J.D. from the Regent University School of Law.

He is excited to be a Texan and lives in Hays County with his wife and two kids.

Texas Public
POLICY FOUNDATION

901 Congress Avenue | Austin, Texas 78701 | (512) 472-2700 | www.TexasPolicy.com