Deepfakes: The Legal Implications

By: Jeffrey Caleb Hendrix

With artificial intelligence consistently improving, the ease of creation and the realistic nature of deep fake media have become a bigger legal problem[1]. Experts in the field define Deepfakes as videos, images, even audio files generated or manipulated by artificial intelligence to depict something that never occurred, in a realistic manner[2]. Further, they add that these types of images are produced through the reliance on copious amounts of data to find and reconstruct the facial features of specific individuals[3]. More technically, experts from Thompson Reuters explain that creating deepfakes typically involves using two generative AI (GenAI) tools within a generative adversarial network (GAN) – a generator (encoder) and a discriminator (decoder). They describe the feedback loop between these tools, where the generator creates artificial outputs and the discriminator tries to detect them, leading to increasingly realistic deepfakes. Id at 2.

Most importantly, experts across this research establish that deep fakes are infiltrating areas that must be preserved, such as our youth, our elections, financial fraud, individuals' ability not to be harassed, and even national security. Id at 3. Experts even added that a deceptive or fraudulent deepfake could seemingly depict a candidate portraying a message that injures their reputation to deceive voters[4]. Further, new AI tools allow individuals to create full videos of situations that never occurred and use this content for their unethical gain. Id at 3.

The use of software to create these images has exploded, and there are currently applications using AI to facilitate the creation of hyper-realistic nude images without consent, simply from an ordinary photo of the party[5]. Now, the effect of this material is harsh; victims reported anxiety, depression, and in extreme situations, committed suicide due to being exploited by an individual utilizing one of these entities. Id. Further, individuals clarify that job loss due to nonconsensual explicit

[1] https://www.nbcnews.com/politics/congress/house-passes-bipartisan-bill-combat-explicit-deepfakes-trump-rcna203316
[2] https://www.thomsonreuters.com/en-us/posts/government/deepfakes-federal-state-regulation/
[3] https://ballotpedia.org/AI_deepfake_policy_in_South_Carolina
[4] https://www.scstatehouse.gov/sess126_2025-2026/bills/3517.htm
[5] https://www.forbes.com/sites/kimelsesser/2025/05/19/new-take-it-down-law-will-protect-against-deepfake-nudes/

materials, whether deepfake or nonconsensual intimate image sharing, is much more common than it is covered. Id. The effect this has on the women of this country is disproportionate, with the American Sunlight project finding that women lawmakers are seventy times more likely to be targeted by intimate imagery non-consensually. Id. This same research highlighted that one in six congresswomen has already become a victim of AI-generated content. Id. Overall, experts from Forbes agree that this field has expanded, and there is minimal evidence of self-regulation within the industry[6]. Further, these tools create significant legal risks and new questions to be answered in the world of defamation, intellectual property, and, of course, blackmail. Id at 2. Nonetheless, we have seen legislative efforts in the last months by both the Federal and State governments to prevent this abuse from persisting and address these new problems with new laws[7].

Federal Legal Landscape: The Take It Down Act and Related Measures

The Federal Government has been adamant about pushing through legislation that allows its prosecutors to combat this growth. Id. Most recently, the federal legislature passed an act known as the "TAKE IT DOWN" act with incredibly strong support from both parties, where the final vote in the House was an overwhelming 409-2. Id. at 1. Following such, this act was passed unanimously in the Senate and signed into law by President Trump on May 19, 2025. Id. at 1. Internally, the act criminalizes the publication of nonconsensual sexually explicit images and videos online, including those generated by AI[8]. The Act requires online platforms to remove such content within 48 hours of notice from the victim. It criminalizes the publication or threat to publish non-consensual intimate imagery (NCII) in interstate commerce. Id. The law protects good faith efforts to aid victims by permitting disclosure for law enforcement or medical treatment purposes[9]. Further, the TAKE IT DOWN Act is noted as the first U.S. law to substantially regulate a certain type of AI-generated content. Id. This act imposes penalties for individuals who post content violating the constraints, including fines or up to three years

[6] https://www.forbes.com/councils/forbestechcouncil/2025/04/17/face-off-how-deepfake-identities-are-rewriting-the-rules-of-financial-crime-and-why-compliance-must-catch-up/
[7] https://www.nbcnews.com/politics/white-house/trump-sign-bill-cracking-deepfake-pornography-rcna207693
[8] https://apnews.com/article/take-it-down-deepfake-trump-melania-first-amendment-741a6e525e81e5e3d8843aac20de8615
[9] https://www.mintz.com/insights-center/viewpoints/54731/2025-05-02-congress-passes-ai-deepfake-law-trump-signs-eo-ai

in prison, while platforms that fail to comply may face enforcement from the Federal Trade Commission. Id at 5. However, some experts raised that the FTC overseeing enforcement may reduce the act's effectiveness due to their manpower being substantially weakened by cuts and restrictions imposed by the current administration[10]. Nonetheless, anyone who persists in intentionally distributing explicit images without consent will face up to three years in prison. Id at 9. In addition, the accountability extends civilly to provide liability for online platforms that refuse to take these images down upon request. Id. at 1

In other news, there is currently a proposed budget reconciliation package including measures such as a 10-year ban on state AI regulations recently passed by the House[11]. Here, House Republicans supported this ban to avoid a "patchwork" of state laws that could hinder innovation and business. Id. Further, the advocates for this establish that through Congress developing the policy, there would be uniformity nationwide in compliance. Id at 9. Accordingly, a moratorium barring state policy would place the burden on Congress and the president to ensure that they expand their deep fake legislation to encompass and address other threats not directly affected by the Take It Down law now in effect. Id at 2. However, South Carolina's own Attorney General Alan Wilson has joined upwards of forty state attorneys general in strongly opposing this proposal, drafting a letter to the speaker of the U.S House, the Senate Majority Leader, the House Minority Leader, and the Senate Minority Leader directly opposing the AI restrictions of this bill[12]. These professionals establish that states have already begun enacting and are still considering legislation to address many avenues of potential AI harm, and that this bill would erase protections created by the state without guaranteeing a federal regulation, which could leave their constituents at risk[13]. Rather than restricting states and attempting to regulate all AI in Congress, they call for collaboration where the federal government should focus on high-risk systems and encourage transparency and enforcement. Id. Nonetheless, Wilson says this one-size-fits-

[10] https://www.nytimes.com/2025/05/22/business/media/deepfakes-laws-free-speech.html
[11] https://www.mintz.com/insights-center/viewpoints/54731/2025-05-16-us-copyright-office-releases-third-report-ai
[12] https://wpde.com/news/local/federal-overreach-ag-wilson-pushes-back-on-bill-to-limit-ai-regulation-for-a-decade-alan-wilson-artificial-intelligence-mike-johnson-john-thune
[13] https://www.scag.gov/media/opvgxagq/2025-05-15-letter-to-congress-re-proposed-ai-preemption-_final.pdf

all mandate from Washington is not leadership but rather federal overreach that could leave state citizens at risk while legislation is handicapped. Id. at 12.

South Carolina's Response: State Legislation and Proposals

Despite the pending bill, which would enact a moratorium on Artificial Intelligence regulation by states, South Carolina has recently established two laws that constrain the use of this software to create lewd material featuring any depiction of a non-consenting individual. Id at 3. Following the signature from the state's governor, it is now a felony in South Carolina to create, distribute, or possess AI-generated sexual images, including child sexual abuse material (CSAM). Id at 3. The state's attorney general, Alan Wilson, establishes that these two new bills "give us the teeth" they require to go after these individuals who are using AI tools to create fake pornography depicting real people, which he establishes as primarily affecting the women and children of our state[14]. Further, Wilson adds that the bills will close loopholes in the prosecution of AI-generated CSAM, as this law expands even to depictions without an identifiable minor. Id. Accordingly, experts believe this is a major step forward in enabling the state of South Carolina's authorities to pursue criminal charges against these individuals, which they were handicapped from doing prior. Id. Further, Attorney General Wilson believes these bills make South Carolina a model state in combating AI-driven exploitation, establishing that the state will take proactive steps to mitigate these risks. Id.

Nonetheless, there are still gaps in South Carolina's legislature related to deepfakes usage in elections, which are to be addressed in House Bill 3157, which has not yet been enacted. Id. at 4. This bill, titled Deceptive and Fraudulent Deepfake Media in Elections, was introduced in January of 2025 and is currently held up in the Committee on Judiciary. Other advocates establish that while these bills are a step in the right direction for preventing exploitation, the state was still lacking a nonconsensual intimate image sharing statute that would bar images originally shared consensually from being distributed out of spite[15]. As such, while drafting this article, South Carolina House Bill 3049 was

[14] https://abcnews4.com/news/local/lawmakers-pass-bill-making-ai-generated-child-sexual-abuse-material-a-felony-alan-wilson-csam-morphed-images-deepfake-artificial-intelligence
[15] https://www.scstatehouse.gov/sess126_2025-2026/bills/3049.html

signed by the State's Governor, Henry McMaster, on May 29th of 2025, officially addressing intentional and threatened disclosure of intimate images without consent[16]

Looking Forward: Further Legislative Safeguards

While legislation like the federal TAKE IT DOWN Act and South Carolina's recent bills address critical areas like explicit deepfakes, multiple challenges remain[17]. Concerning South Carolina, despite the recent bills giving prosecutors the ability to address this type of material as it relates to children and non-consenting adults, the potential for exploitation does not end there. South Carolina was currently one of the only states that still did not have a nonconsensual intimate image sharing statute, which bars individuals from sharing sexually explicit images without consent and out of spite, but no longer. Id. at 14. Moreover, the specific restrictions presented by the proposed SC election deepfake bill (H.3517) will prohibit the use of deceptive deep fake or synthetic material within ninety days of an election that does not disclose the content has been manipulated or generated from AI[18]. If this gets enacted, the criminal penalty for such acts will be a misdemeanor with potential imprisonment and a fine for a first offense, with escalation to a felony with longer imprisonment and a higher fine if a second offense occurs within five years. Id. Further, there are civil actions available to a candidate whose likeness is portrayed, as they can seek injunctive and equitable relief as well as pursue an action for damages. Id. Nonetheless, these protections will not be available for upcoming elections if the legislation is not passed before a potential federal moratorium is imposed.

Likewise, the Federal government has several pending related bills that would combat risks, such as the NO AI Fraud Act, which seeks to establish specific property rights over an individual's physicality, including their voice, to combat unauthorized AI-generated replica content[19]. Further, the Federal government has legislation pending that would attempt to combat the election issue, with the Protect Elections from Deceptive AI Act, which would prohibit the distribution of deceptive AI

[16] https://www.wistv.com/2025/05/29/governor-holds-ceremony-sign-revenge-porn-bill-into-law/
[17] https://salazar.house.gov/media/press-releases/us-senate-passes-salazars-bill-protect-deepfake-revenge-porn-victims
[18] https://www.scstatehouse.gov/sess126_2025-2026/bills/3517.htm
[19] https://salazar.house.gov/media/press-releases/salazar-introduces-no-ai-fraud-act#:~:text=Mar%C3%ADa%20Elvira%20Salazar%20(R%2DFL,AI%2Dgenerated%20fakes%20and%20forgeries.

generative audio or visual media as it relates to federal candidates[20]. Also, one additional piece of legislation pending is titled the AI Transparency in Elections Act, which would require disclaimers on political advertisements including AI-generated content, nonetheless, neither of these has gotten traction past the Senate Rules Committee[21].

Additionally, the rapid evolution of financial crime, particularly through synthetic identities generated by deepfakes, is outpacing regulators and compliance teams[22]. As such, financial institutions face billions in potential losses from AI-driven fraud. Id. Accordingly, deepfake detection is noted as an overlooked gap in fraud prevention strategies, as traditional KYC ("Know your customer")/AML (Anti-Money Laundering) programs designed for human fraudsters struggle against AI-generated identities that can bypass checks and mimic legitimate behavior. Id. For financial institutions, Parya Lotfi of Forbes Technology Council recommends embedding deepfake detection into KYC and fraud prevention workflows to preempt synthetic identity fraud before accounts are approved. Id. Further, they also advise conducting deepfake audits as part of AML compliance reviews and leveraging AI-driven solutions that can adapt to evolving deepfake threats. Id.

Similarly, another place where experts are highlighting that deepfakes can create risk for citizens is the world of business email compromise, with evidence of these attacks being present in all fifty states as of 2023[23]. Further, U.S bank experts clarify that the development of deepfake audio is allowing cybercriminals to execute elaborate business email compromise frauds via phone or video[24]. They establish that Deepfake audio is a form of voice swapping achieved by using a machine-learning algorithm to mimic the voice of a real person, either on the phone or through a video. Id. Further adding that the most advanced hackers can create a voice profile of an individual with less than twenty minutes of audio and then pair this with a script to probe for sensitive information within a company

[20] https://www.congress.gov/bill/118th-congress/senate-bill/2770
[21] https://www.klobuchar.senate.gov/public/index.cfm/2024/3/klobuchar-murkowski-introduce-bipartisan-legislation-to-require-transparency-in-political-ads-with-ai-generated-content
[22] https://www.forbes.com/councils/forbestechcouncil/2025/04/17/face-off-how-deepfake-identities-are-rewriting-the-rules-of-financial-crime-and-why-compliance-must-catch-up/
[23] https://www.ic3.gov/PSA/2024/PSA240911
[24] https://www.usbank.com/financialiq/improve-your-operations/minimize-risk/bec-and-deepfake-fraud.html

or individually. Id. Primarily, one FINCEN report highlights these schemes themselves typically involve criminals using compromised or spoofed accounts, masked to appear as belonging to company leadership, vendors, or lawyers, in an attempt to trick employees with access to company finances into transferring funds or sharing sensitive information to accounts believed to belong to trusted partners, and the use of Deepfakes adds a layer of realistic impersonation through manipulated audio or video[25]. Accordingly, FBI and U.S. bank experts go on to recommend raising awareness of the possibility of these attacks, as well as training staff to be wary of unusual or urgent requests, and, most importantly, always confirming suspicious communication, especially involving money or sensitive information, through trusted contact methods with superiors. Id at 24.

Finally, lawmakers and advocates are still balancing concerns about deepfakes with First Amendment free speech considerations and beneficial uses of the technology. Id. at 3. Additionally, digital rights groups have raised issues that some legislative measures could threaten free speech and privacy rights. Id. at 1. Accordingly, while awaiting news on whether all regulation of artificial intelligence tools will remain the Federal government's responsibility solely, South Carolina's attorney general has established that collaboration remains key to addressing this issue, and that this state's recent efforts could serve as a model for addressing the use of artificial intelligence to harm individuals through deepfakes and combat these concerns within their municipalities. Id. at 2.

[25] https://www.fincen.gov/sites/default/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf