The Regulatory Review
A Publication of the Penn Program on Regulation

Seminar | Rights | Jun 14, 2025

Reckoning With the Rise of Deepfakes

Grace Schuette, Atinuke Lardner, and Evelyn Woo

Scholars explore deepfakes' evolving capabilities and propose methods for regulating them.

The Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act (TAKE IT DOWN Act), enacted on May 19, 2025, is the first federal statute that criminalizes the distribution of nonconsensual intimate images, including those generated using artificial intelligence (AI), known as

"deepfakes."

The first known deepfakes—synthetic images, audio, and videos that look hyper-realistic and depict real or fictional individuals—appeared on Reddit, an online discussion platform, in 2017 when a user posted pornographic videos with the faces of female celebrities superimposed on other bodies. Deepfakes are created using advanced machine learning techniques designed to produce content that is often indistinguishable from real media.

Deepfakes can have many beneficial uses. In medicine, deep learning algorithms can locate cancerous tumors with a high level of accuracy and even predict whether cancerous regions have spread. In education, deepfakes can resurrect historical figures to deliver interactive lessons, fostering engagement in classrooms and museums.

Although developers have adapted deepfake technology to support industries such as health care, marketing, and entertainment, the vast majority of deepfake videos involve sexually explicit content. Creators of deepfakes disproportionately target women and minors, raising concerns about privacy and abuse.

Some scholars warn that the spread of deepfakes threatens both individual privacy and public trust in information. Deepfake technology has already been used to depict political figures delivering fabricated speeches and engaging in fictional misconduct, raising alarms about its potential to undermine democratic institutions. The hyper-realism of deepfake content makes it difficult for the public to distinguish what is real and what is not, further disseminating disinformation and reducing confidence in legitimate media.

Before the TAKE IT DOWN Act, states individually regulated AI-generated intimate imagery. As of 2025, all 50 states and Washington, D.C. have enacted laws targeting nonconsensual intimate imagery, and some have updated their language to include deepfakes. These laws, however, vary in scope and enforcement.

The TAKE IT DOWN Act addresses the gaps left by state laws at the federal level. The Act prohibits the distribution of nonconsensual intimate images, including AI-generated ones, with penalties of up to two years' imprisonment. The Act also requires online platforms that host user-generated content to establish notice-and-

takedown procedures that require removing flagged content within 48 hours and deleting duplicates. The Federal Trade Commission may enforce these provisions against platforms that fail to comply.

Many scholars agree on the need to regulate harmful deepfakes, but critics warn that broad laws could infringe on First Amendment rights, especially in satire or political speech. Legal scholars debate how to address deepfakes' harms without undermining protected expression. As deepfake technology advances, lawmakers must decide how to curb its most damaging uses without sacrificing free speech or stifling innovation.

In this week's Saturday Seminar, scholars consider the legal and technological challenges of regulating deepfake content.

- In an article in *The Jurisprudence*, Andrew Street of Southern University Law Center examines the recent prevalence of deepfakes and proposes regulating them through right-of-publicity ("ROP") frameworks. Street argues that intellectual property law may offer the most balanced approach, mitigating harm from deepfakes while preserving First Amendment protections through fair use provisions. Street notes that trademark and copyright law fall short because they target commercial use and do not grant a proprietary interest in one's own identity. ROP, by contrast, can address nonconsensual uses of a person's likeness that fall outside protected speech, says Street recommends a narrowly tailored federal ROP that ensures free speech and technological innovation while preventing harmful deepfake content from proliferating.
- In an article in the *Journal of Law and Society*, Clare McGlynn, of the United Kingdom's Durham University Law School , and Rüya Toparlak, of the Switzerland's University of Lucerne, consider the harms inherent in creating sexual deepfakes and argue that laws should target the creation of deepfakes in addition to the distribution. Framing creation as a form of "new voyeurism," McGlynn and Toparlak emphasize that the creation of deepfakes is wrong and harmful itself, even without distribution or victim knowledge, because it violates bodily autonomy and appropriates one's likeness for nonconsensual sexual use. They also recommend the term "sexual digital forgeries" instead of "deepfake pornography" to capture the fraudulent and nonconsensual nature of the content more accurately.

- In a forthcoming article in the *Arizona State Law Journal*, Michael Goodyear of New York University School of Law analogizes the current legal dilemma presented by deepfakes to the advent of the camera. Goodyear contends that ROP, which evolved in response to unauthorized use of photographed likenesses, can address the proliferation of deepfakes, which Goodyear argues threatens human dignity. Goodyear explains that unlike most proposed legal remedies, ROP would oblige online platforms to adopt notice and takedown measures, which interrupt the dissemination of deepfakes. Goodyear acknowledges that users may view content briefly, but maintains that the policies benefit victims by addressing both commercial and dignitary harms of deepfakes. Goodyear recommends legislation extending ROP to hold platforms liable for hosting deepfake content.
- In a forthcoming article in the *University of Pennsylvania Journal of Constitutional Law*, Hillary B. Farber and Anoo Vyas of the University of Massachusetts School of Law, argue that modern interrogation law lacks clear constraints on using generative AI to fabricate evidence. Farber and Vyas note that unlike traditional "false evidence" lies, AI-generated deepfakes exponentially amplify coercion in custodial settings, yet no statutory or judicial decision expressly prohibits their practice. They recommend that courts extend existing due-process safeguards by adopting a bright line rule that deems any confession extracted through AI-fabricated evidence involuntary and inadmissible under the Fifth and Fourteenth Amendments. They contend that this standard would strengthen procedural fairness and deter AI misuse in interrogations.
- In a forthcoming article in the *Law Review of the Franklin Pierce Center for Intellectual Property*, Michael Murray, of the University of Kentucky College of Law, argues that lawmakers can use existing legal frameworks, namely ROP, right of privacy, and trademark law to regulate deepfakes. Murray explains that ROP protects against unauthorized commercial use of AI-generated likenesses and that privacy law can apply when deepfakes invade an individual's private life, though expressive uses like parody may be protected by the First Amendment. Murray describes how trademark law can be deployed against AI-generated false endorsements by public figures. Murray recommends using existing legal frameworks as a guideline for addressing the harms caused by evolving deepfake technology.
- In an article in *Psychology and Education: A Multidisciplinary Journal*, Jan

Mark S. Garcia of West Visayas State University argues that deepfake creators exploit gaps in regulatory frameworks and undermine accountability. Although some governments have criminalized deepfakes used for fraud or harassment, Garcia emphasizes that enforcement remains difficult without a global regulatory consensus. Garcia warns that inadequate governance of deepfake technology poses serious threats to individuals, businesses, and political institutions. Garcia calls for stronger, deepfake-specific regulations and urges collaboration among governments, technology companies, and researchers to establish clear ethical guidelines. Garcia highlights the urgent need for coordinated regulatory efforts to address the fast-evolving challenges posed by synthetic media technologies.

The Saturday Seminar is a weekly feature that aims to put into written form the kind of content that would be conveyed in a live seminar involving regulatory experts. Each week, *The Regulatory Review* publishes a brief overview of a selected regulatory topic and then distills recent research and scholarly writing on that topic.

Tagged: AI, Deep Fake, First Amendment