

Policy Backgrounder

Me, Myself, and IP: AI and the Deepfake Problem

A recent AI deepfake incident involving NVIDIA CEO Jensen Huang highlights the growing challenge that businesses and policymakers have in responding to the rapid spread of highly realistic synthetic media that can deceive the public and erode trust. A proposed law in Denmark would give individuals copyright over their personal characteristics and prohibit sharing of deepfakes without consent.

Trusted Insights for What's Ahead®

- Organizations should evaluate their exposure to deepfake-related threats and implement safeguards to mitigate risks. These may include reputational damage from fabricated or misleading media as well as financial losses from scams that deceive employees or customers.
- Leaders should also train employees to recognize deepfakes and strengthen protocols and technical tools for verifying the authenticity of directives and information.
- CEOs should also engage their media and legal teams to carefully monitor abuse of their likeness and prepare to respond quickly when incidents occur.
- Both Congress and several states have enacted laws attempting to address certain kinds of deepfakes, such as nonconsensual intimate photos and using deepfakes to further the commission of a crime.
- Danish lawmakers are considering a novel approach that would grant individuals copyright over their own personal characteristics (such as appearance and voice) and prohibit the sharing of deepfakes without consent regardless of whether harm was done.

The Deepfake Problem

When NVIDIA CEO Jensen Huang took to the stage to deliver the keynote [address](#) at a recent company conference, those streaming the address online should have heard him discuss NVIDIA's outlook for quantum computing, AI, robotics, and other topics. However, nearly 100,000 people instead [saw](#) a different address in which an AI-generated deepfake of Jensen Huang promoted cryptocurrency scams. Though YouTube eventually removed the fake video, at one point more than eight times as many people were streaming the fake video as the real one.

The incident highlights a growing [problem](#) for individuals, businesses, and governments as generative AI has dramatically lowered the cost and effort required to produce hyper-realistic fake photos, videos, and audio – often called “synthetic media.” In 2024, for example, an employee at a UK engineering firm was [tricked](#) into sending \$25 million to scammers after a video call with a deepfake version of the company's CFO and other colleagues. Experts have also expressed [concerns](#) about the effect on evidence authenticity in legal proceedings and about how [deepfakes](#) of political and military leaders could lead to [geopolitical](#) instability and conflict.

Existing Policy Landscape

As deepfakes and other forms of synthetic media proliferate, governments around the world are struggling to adapt existing legal frameworks to a rapidly changing technological reality. The laws that govern intellectual property, privacy, and defamation were not designed for an era in which anyone can fabricate realistic video, audio, or images at scale. Policymakers have therefore begun experimenting with new approaches – some focused on criminal penalties, others on transparency and labeling requirements, and still others on expanding individual rights to control one's likeness. Yet these efforts remain uneven across jurisdictions, reflecting different legal traditions and cultural attitudes toward speech, privacy, and innovation.

United States

The US Congress [passed](#) the Take It Down [Act](#) in May 2025, the first Federal law to target the online publication of nonconsensual intimate visual depictions of individuals, both authentic and computer-generated. Also on the Federal level, in 2023, the Federal Election Commission (FEC) initiated a rulemaking process to potentially regulate deepfakes in political ads; however, due to [disagreements](#) about whether the FEC had the authority to issue such a regulation, it instead opted to [issue](#) an Interpretive Rule clarifying that deepfakes fall under existing election law barring fraudulent misrepresentation. Some then-Commissioners [expressed](#) hope that Congress would legislate a more comprehensive solution. However, other kinds of deepfakes, such as non-intimate impersonations, voice-cloning fraud, political election-deepfakes or economic harm misuses, remain [governed](#) by a patchwork of state laws and broader tort or criminal frameworks. Yet these general-purpose laws were not designed for synthetic media and often leave [gaps](#) in coverage and enforcement.

Some US [states](#) have attempted to fill these gaps. For example, Tennessee's 2024 Ensuring Likeness, Voice, and Image Security (ELVIS) [Act](#) extended existing prohibitions on unauthorized commercial use of an individual's name, image, and likeness to include their voice. The ELVIS Act also targets AI platforms by creating a legal liability for firms that provide technologies "the primary purpose or function of which is the production of an individual's photograph, voice, or likeness without authorization from the individual." Likewise, a 2025 New Jersey [law](#) makes it a crime to create or knowingly disclose "a work of deceptive audio or visual media for the purpose of attempting or furthering the commission of any crime or offense." However, in some cases such laws are legally vulnerable under the First Amendment and Section 230 of the Communications Decency Act of 1996. For example, in October 2024 and August 2025, a Federal judge struck [down](#) two California laws that would have imposed restrictions on political deepfakes during elections and penalties for online platforms that do not label or block them. Policy [debates](#) also reflect [uncertainty](#) about how to balance [tensions](#) between the principles of free expression and the importance of preventing deception, reputational harm, and public mistrust fueled by deepfakes.

European Union

In contrast to the US, in May 2024, the European Union (EU) adopted the West's – and arguably the world's – first comprehensive AI law, the Artificial Intelligence [Act](#), establishing a legal framework for governing AI models developed or deployed in the EU. Among other provisions, the Act requires that content that is created or modified using AI be clearly labeled as such. In addition, in September Italy became the first EU member state to enact a comprehensive law, [designed](#) to complement the EU AI Act, regulating the use of AI, which includes penalties for generating or spreading malicious deepfakes.

Denmark is [reportedly](#) considering a novel approach that goes beyond disclosure and penalties for malicious content. According to a [proposal](#) released by the Danish Ministry of Culture [amending](#) the country's Copyright Act, Danish law may soon grant individuals copyright over their own personal characteristics (such as appearance and voice) and prohibit the sharing of realistic, digitally-generated imitations without consent regardless of whether harm occurred. Legal experts [note](#) that this would mark a significant expansion of the traditional interpretation of copyright, which typically protects human creative works such as songs and books, and may have unintended consequences. They also raised [concerns](#) about how the protections would be enforced, legal [risk](#) for firms that use facial recognition technology, and potential infringements on free speech. Others point out that the proposal reflects frustration that social media platforms rarely respond to requests to remove content without a legal threat.

Denmark's Parliament, the Folketing is expected to consider the proposed law this Fall; it has broad support and is expected to come into force by next year. By considering the deepfakes as "illegal content," the law would trigger the mandatory removal provisions of the EU's Digital Services Act.

Policy Outlook

The divergence between the US and EU regulatory approaches underscores broader differences in regulatory philosophy. Whereas the US has tended to focus on addressing specific deepfake [harms](#), sometimes constrained by the First Amendment, the EU has favored a framework that imposes proactive obligations on platforms and AI developers to identify, label, and mitigate risks associated with synthetic media. These differences may create practical challenges – both for firms seeking to comply with differing requirements across borders, but also for enforcement as digital content moves easily across the globe.

The regulatory efforts also reflect the ongoing challenge policymakers have in responding to a quickly evolving technological landscape with unknown future consequences. Some firms and [organizations](#) are attempting to develop technical solutions such as digital watermarking and content authentication standards that aim to detect deepfakes or verify the authenticity of photos and videos. Even when created consensually, AI-generated content can raise thorny consumer protection issues. For example, a US actor who licensed his likeness to TikTok has [expressed](#) regret that his digital avatar is now being used to advertise for a range products including insurance and a horoscope app.

The spread of deepfakes illustrates the growing tension between technological innovation and the legal, ethical, and social systems meant to govern it. While policymakers in the US, EU, and elsewhere are beginning to respond, their efforts remain fragmented and often reactive to emerging harms rather than anticipatory of future risks. The debate over how to regulate synthetic media reflects broader questions about identity, accountability, and truth in the digital age – questions that test the limits of existing frameworks for privacy, speech, and intellectual property. As generative AI continues to evolve, societies must grapple with the reality that the authenticity of what we see and hear can no longer be taken for granted.

About the Authors



David Young, President, CED



John Gardner, Vice President, Public Policy, CED



PJ Tabit, Principal Economic Policy Analyst, CED

THE CONFERENCE BOARD is the Member-driven think tank that delivers *trusted insights for what's ahead*®. Founded in 1916, we are a nonpartisan, not-for-profit entity holding 501(c)(3) tax-exempt status in the United States.

The Committee for Economic Development (CED) is the public policy center of The Conference Board. The nonprofit, nonpartisan, business-led policy center delivers trusted insights and reasoned solutions in the nation's interest. CED Trustees are chief executive officers and key executives of leading US companies who bring their unique experience to address today's pressing policy issues. Collectively, they represent 30+ industries and over 4 million employees.

© 2025 The Conference Board, Inc.