Forged Faces, Real Liability: Deepfake Laws Take Effect in Washington State and Pennsylvania

Client Alert | 4 min read | 08.19.25

In the last few months, both Washington State and Pennsylvania enacted significant legislation addressing the malicious use of deepfakes—artificial intelligence-generated or manipulated media. These new laws reflect a growing national and state-level trend to regulate AI-generated content, especially when used to harm individuals or mislead the public.

On July 7, 2025, Pennsylvania Governor Josh Shapiro signed into law Pennsylvania's 2025 **Act 35** (formerly Senate Bill 649), which establishes criminal penalties for creating or disseminating deepfakes with fraudulent or injurious intent, or facilitating a third party to do so. This includes when a party reasonably should have known the material at issue was a forged digital likeness. The law, which goes into effect on September 5, 2025, classifies such conduct as a first-degree misdemeanor ($1,500 - $10,000 fine and/or up to five years jail time), or a third-degree felony (up to $15,000 fine and/or up to seven years jail time) when done to "defraud, coerce or commit theft of monetary assets or property." This portion of the law targets impersonation, financial scams, or election-related deception as many older adults in the state have fallen victim to scams this past year. While the new law is rooted in protecting individual privacy and public trust, it also includes carve-outs for protected expression, such as satire or content in the public interest, as well for technology companies that provide the means to create the deepfakes, and the information service providers who disseminate the content, as long as they did not intentionally facilitate its creation and dissemination. It also is a defense to place a disclaimer on the digital content that the digital likeness is fake. This law builds upon earlier Pennsylvania statutes that criminalize the non-consensual distribution of AI-generated sexual imagery, and it follows recent enforcement activity involving deepfake content used to depict minors in explicit material.

Similarly, in Washington State, **House Bill 1205** went into effect on July 27, 2025, which criminalizes the intentional use of a "forged digital likeness"—including synthetic audio, video, or images—when done with the intent to "defraud, harass, threaten, or intimidate another or for any other unlawful purpose." This includes when a party knew or should have known the forged digital likeness was fake. Violations are classified as gross misdemeanors, punishable by up to 364 days in jail and a $5,000 fine, with more serious penalties possible in cases involving fraud or identity theft. Notably, the law includes exemptions for "matters of cultural, historical, political, religious, educational, newsworthy, or public interest", and for platforms (e.g. interactive computer services and telecommunications providers) that promptly respond to takedown requests, thereby attempting to balance enforcement with First Amendment protections.

These developments align with a broader **national movement**, with dozens of states adopting laws to regulate deepfakes that criminals use to create non-consensual intimate imagery, manipulate elections, or conduct fraud. In May 2025, President Trump signed the most far-reaching federal legislation on this subject, the **TAKE IT DOWN ACT**, which prohibits the nonconsensual publication of intimate visual depictions, including deepfakes, and requires online platforms to remove them if victims give them notice. The Federal Trade Commission may consider a platform’s failure to reasonably comply with the law’s notice and takedown obligations as an unfair or deceptive act or practice.

Several other states have expanded their rights of publicity to protect creators’ from the unauthorized use of their likenesses in deepfakes. For example, in 2024, Tennessee adopted the Ensuring Likeness Voice and Image Security Act (ELVIS Act), which prohibits the use of AI to mimic a person’s voice without their permission.

In light of these developments nationwide, companies should be keenly aware of their use of AI technologies in advertising, content creation, campaign materials, and internal communications. Companies should audit AI-generated content for compliance, review contracts with endorsers and influencers to include provisions regarding the use of AI-technology, train staff to recognize and escalate potential misuse, establish prompt takedown and notice procedures, and update consent protocols for synthetic likenesses. Businesses operating in higher risk sectors—media, entertainment, political advocacy, or consumer-facing AI platforms—should include disclaimer language and consent documentation to mitigate exposure under these new laws. Ultimately, the fact that an individual’s image and likeness is generated by AI likely does not take away from that individual’s right of publicity.

At the same time, trends of targeting company executives with deepfake videos that deceive the public in a variety of ways continue. These laws provide new legal tools that companies may be able to leverage when company executives are targeted by deepfakes.

For tailored guidance, disclaimer templates, or enforcement insights, please reach out for a follow-up briefing.

Contacts

Andrew J. Avsec
Partner
Chicago D | +1.312.840.3260
aavsec@crowell.com

Megan M. Michaels
Counsel
New York D | +1.212.223.4000
F | +1.212.803.4073
mmichaels@crowell.com