Deepfakes, Digital Replicas and Synthetic Performers: Privacy Risks and Compliance in 2026

Deepfakes have moved from novelty to material enterprise risk, reshaping how organizations assess privacy, security, brand integrity and marketing. This technology can erode evidentiary trust, enable impersonation and fraud and expose organizations to right-of-publicity, consumer protection and regulatory enforcement risks in multiple jurisdictions. New legislation governing deepfake transparency and digital-replica protections continue to emerge at the state and federal levels.

Deepfakes, Digital Replicas and Synthetic Performers

Deepfakes are synthetic media created using AI techniques to produce convincing audiovisual content of events that did not occur, which can be weaponized to distort truth, manipulate opinion and blur the line between authentic and fabricated content. New York defines a "digital replica" as a newly created, computer-generated, highly realistic electronic representation readily identifiable as a person's voice or visual likeness embodied in sound recordings, images, audiovisual works or transmissions where the person did not perform or where the performance was materially altered. In parallel, organizations increasingly deploy fully synthetic AI avatars and lifelike virtual models not tied to a real individual (i.e. "synthetic performers").

Privacy and Cybersecurity Risks in Business Settings

Fraud and social engineering. Deepfaked voices and faces can bypass voice authentication and frustrate liveness checks, enabling account takeovers, fraudulent payments and compromise of sensitive information. Video/voice impersonation power advanced phishing techniques designed to collect confidential data, expanding the attack surface for organizations relying on biometric or video-based verification.

Data integrity. Deepfakes also undermine evidentiary reliability and data integrity across compliance functions, making it harder to rely on audiovisual records. Policymakers and researchers warn of a "liar's dividend," in which the mere prevalence of deepfakes enables criminals to dismiss authentic evidence as fake, compounding the challenge for institutions that rely on digital media.

Reputational harm. Employee safety and brand reputation are at risk when fabricated clips target executives or staff, including non-consensual sexual deepfakes that can create hostile-environment exposure and long-lasting harm to victims' dignity, employability and well-being.

Consumer protection. AI avatars and synthetic performers can be misled if they simulate endorsements or experiences a reasonable consumer would attribute to a human.

Right-of-publicity and IP exposure. Synthetic media can capture distinctive persona, voice or protected expression associated with individuals or brands.

New York's Approach to Deepfake Technology

New York has adopted an **aggressive approach** in prohibiting the dissemination of nonconsensual deepfake sexual imagery. More recently, New York has followed up with additional guardrails for the use of deepfake technology in business contexts.

Digital Replicas. Effective Jan. 1, 2025, New York updated its **General Obligations Law** to void any clause in a personal or professional services agreement that authorizes a "new performance by digital replication" of an individual's voice or likeness in place of work the individual would have done in person, if three conditions are met: the clause permits substitution, it lacks a "reasonably specific" description of intended uses, and the individual lacked either counsel-negotiated, clearly and conspicuously presented terms or coverage under a collective bargaining agreement that expressly addresses digital replicas.

Synthetic performers in advertising. Effective June 9, 2026, New York amended its **General Business Law** to require conspicuous disclosure when an advertisement features a "synthetic performer" if the advertiser has actual knowledge of its inclusion. The law imposes civil penalties of $1,000 for a first violation and $5,000 for subsequent violations. Carveouts include exemptions for advertisements of expressive works if consistent with use in the work, exclusion of audio-only ads and exceptions for AI used solely for language translation of a human performer. Media outlets and platforms are generally not liable absent actual knowledge, and Section 230 protections remain undisturbed.

Looking Beyond New York

State law patchwork. Across the U.S., states have expanded name, image, likeness and voice protections, including postmortem rights and, in some cases, secondary liability for distributing cloning tools primarily designed to produce a specific person's image or voice without authorization (e.g., **Tennessee's ELVIS Act**). These statutes typically include expressive-use exceptions and media safe harbors, but definitions, scope and remedies vary. Other states now require organizations to adhere to strict disclosure requirements when publishing AI-generated image, video or audio content (e.g., **California AI Transparency Act**).

Federal outlook. Effective May 19, 2026, the **TAKE IT DOWN Act** will criminalize the knowing publication and certain threats to publish "intimate visual depictions" and "digital forgeries" of identifiable individuals. In the business context, pending Federal proposals such as the **NO FAKES Act** aim to combat unauthorized "digital replicas" of a person's name, image, likeness and voice with a clear private right of action, and a notice-and-takedown safe harbor, paired with express preemption of overlapping state rules while preserving areas like elections and sexually explicit content.

Practical Mitigation and Compliance Guidance

Given the risks posed by deepfakes and recent legislative activity, businesses should consider the following recommendations:

Governance, policy and training. Adopt an AI media policy covering creation, procurement, disclosure, and internal use of synthetic media and digital replicas. Provide training to legal, security, marketing and customer-facing teams to recognize and escalate deepfake risks.

Contracts, consents and scoping for replicas. Obtain specific, written, informed consent from replica subjects that precisely define media, territories, duration, derivative uses, training of AI systems and revocation/audit rights

Advertising and disclosure controls. Build a disclosure checkpoint into creative workflows for ads featuring synthetic performers. Implement plain language labels appropriate to the medium and confirm compliance FTC Guidelines and other authorities before publication.

Identity, security and fraud controls. Assume deepfake-capable adversaries: update phishing detection safeguards, require step-up authentication for high-risk actions and adopt out-of-band verification and code words for unusual payment or data requests.

Deepfakes and digital replicas are increasingly convincing and create interconnected privacy, security, and legal risks across marketing, customer engagement and identity assurance. For more information or assistance with AI governance and privacy compliance, contact **Mario Ayoub** or any member of Bond, Schoeneck & King PLLC's **artificial intelligence** or **cybersecurity and data privacy** practice groups.