

MARCH 14, 2026 | PUBLICATION

"Digital Risk Report," March 2026

[Download the "Digital Risk Report"](#)

INDUSTRY SECTOR

Technology

SERVICE LINE

Technology, Data Privacy,
Cybersecurity & AI

RELATED PROFESSIONALS

C. Jade Davis
Brian C. Focht
Nick Carr
Lloyd J. Wilson

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

The Deepfake Reckoning: When AI Replicates Reality Without Consent

Deepfakes are no longer a fringe internet problem—they are a growing enterprise risk. In February 2026, data protection authorities from 61 jurisdictions issued a rare joint statement warning organizations about the dangers of artificial intelligence (AI) systems capable of generating realistic images and videos of identifiable individuals without consent. The coordinated message from regulators across Europe, North America, Asia, and beyond is clear: existing privacy laws already apply to generative AI, and enforcement is coming.

The concern extends far beyond viral social media manipulation. Regulators are focusing on the misuse of biometric and personal image data, the rapid spread of non-consensual imagery, and the particular risks these technologies pose to children and vulnerable populations. Many jurisdictions already treat the creation of non-consensual intimate imagery as a criminal offense, and regulators are now signaling that organizations deploying AI tools—whether vendors or enterprise users—may share responsibility when these harms occur.

For businesses experimenting with generative AI, the message is straightforward: AI governance is data governance. Organizations developing or deploying image-generation tools are expected to implement safeguards against misuse, ensure transparency about system capabilities, provide mechanisms for individuals to request removal of harmful content, and adopt stronger protections where children's data may be involved.

As AI becomes embedded across marketing, HR, security, and customer engagement platforms, companies must treat the replication of human likeness—faces, voices, and identities—as highly sensitive data processing. Our team continues to explore what this global regulatory alignment means for organizations deploying generative AI and the practical governance steps privacy, security, and operational teams should be taking now.

Insights in the March 2026 issue include:

- Delaware Supreme Court Expands Cyber Liability Exposure for SaaS & Managed Service Providers
- Your Outside Counsel Is Using AI. Should Your Legal Spend Be Going Down?
- The Artificial Intelligence Benchmark: The Most Important Clause You've Never Used (Part 2)
- Client Alert: New Federal Policy Could Unlock Alternative Water Supplies for Data Centers
- Legislative & Regulatory
- Enforcement Actions
- Notable Data Breaches

Learn more about Shumaker's Technology, Data Privacy, Cybersecurity & AI Service Line