5 KEY TAKEAWAYS

Lies. Truths. Bots: Managing Misinformation, Deepfakes, and Reputational Risk

Artificial intelligence has fundamentally changed the information environment. Convincing deepfakes can impersonate corporate executives, coordinated bot campaigns can manufacture the appearance of widespread public outrage, and false allegations can reach millions before an organization has an opportunity to establish the facts.

For businesses, these are no longer just public relations challenges. They present significant legal, operational, and governance risks.

In a recent CLE program with Jackson Spalding's reputation management and digital analytics leaders, Kilpatrick partner Michael Breslin explored how legal counsel can help organizations navigate these emerging threats. Five practical takeaways emerged:

1

Prepare for a disinformation crisis before it happens.

Companies have invested heavily in cybersecurity incident response plans, but many have no comparable protocol for responding to deepfakes, viral misinformation, or coordinated reputational attacks.

Outside counsel can help organizations build that playbook: establishing response teams, defining escalation triggers, developing evidence-preservation procedures, and coordinating legal, communications, cybersecurity, and executive decision-making. The first hour of a crisis is not the time to determine who has authority to investigate, speak, or act.

2

Don't confuse authentic-looking information with the truth—or fabricated content with false allegations.

A convincing video can be entirely fabricated. An authentic recording can be selectively edited to create a misleading impression. And even a fabricated whistleblower or coordinated bot campaign can circulate allegations that are substantively true.

Legal counsel must distinguish three questions: Is the material authentic? Are the underlying allegations accurate? And what can the organization responsibly substantiate in its response?

Failing to separate those questions can turn a manageable reputational incident into a much larger legal problem.

3

Modernize identity verification, corporate controls, and insurance coverage for the deepfake era.

AI-generated voices and video can convincingly impersonate executives, employees, and trusted business partners. Traditional safeguards that depend on recognizing someone's face or voice are increasingly inadequate.

Companies should establish independent verification procedures for sensitive instructions, including callbacks to previously authenticated contacts, secure authorization channels, and dual approval for high-value transactions. They should also **review existing cyber, crime, and other potentially applicable insurance policies** to determine whether losses resulting from deepfake impersonation, fraudulent transfers, or related incidents are covered—and identify exclusions, conditions, or coverage gaps before an incident occurs.

The governing principle: Authenticate the person independently, authorize the transaction separately, and understand your insurance protection before you need it. Outside counsel can help assess whether existing safeguards and coverage are appropriate given the organization's particular risks, contractual obligations, and regulatory environment.

4

Respond quickly—but don't let the public narrative get ahead of the facts.

In a viral crisis, communications professionals understandably prioritize speed. Lawyers must also consider accuracy, preservation obligations, privilege, regulatory exposure, and the potential consequences of public statements in future litigation. Those priorities need not conflict. Organizations can promptly acknowledge an incident, explain that an investigation is underway, and communicate verified information without making categorical assertions they cannot yet support.

The best immediate communications strategy is not always the best long-term legal strategy. A public statement that wins the news cycle can become a damaging exhibit in litigation if subsequent evidence contradicts it.

5

Recognize that the lawyer's role is to protect the client's credibility—not simply defend its preferred narrative.

When executives believe their organization is being unfairly attacked, their instinct may be to respond aggressively, deny allegations unequivocally, or pursue legal action against those responsible. Outside counsel provides particular value by exercising independent judgment: testing the client's assumptions, evaluating the available evidence, identifying legal remedies, and considering whether the proposed response will advance the client's long-term interests.

As Georgia's Aspirational Statement on Professionalism recognizes, lawyers serve as advocates for clients to the public and as an independent voice counseling clients about their conduct. **Effective crisis counsel does more than determine what a company can say or do. It helps leadership determine what the company should say or do—and when.**

The Bottom Line

Misinformation, disinformation, and synthetic media should be treated as enterprise risks, not simply communications problems. Organizations that integrate legal, technical, and reputational expertise before a crisis will be better positioned to respond decisively, preserve their options, and protect their credibility when the facts are contested.

Michael Breslin is a partner at Kilpatrick and a leader of Kilpatrick Connect, the firm's multidisciplinary initiative focused on AI governance and risk management. His practice includes complex commercial litigation, technology-related disputes, and counseling businesses on emerging legal and operational risks.

For more information, please contact:
Michael Breslin: mbreslin@ktslaw.com

www.ktslaw.com