PULLMAN & COMLEY

AI Deepfakes in the Workplace: A New Frontier of Employer Liability

Working Together

03.09.2026

By Ryan O'Donnell

The technology that was supposed to make work easier is now making it more dangerous. AI-generated deepfakes—defined generally as fabricated images, video, and audio that look and sound real—have arrived in the workplace, and they're creating a category of liability that didn't exist two years ago.

For employers, especially those in hospitality and other high-turnover industries, the message is straightforward: your current handbook probably doesn't address this. It needs to.

What's Happening

Employees are using AI tools to create doctored images and audio targeting coworkers. The content ranges from sexually explicit deepfakes to fabricated recordings designed to humiliate or defame. Recent lawsuits illustrate the scope of the problem.

For example, a 19-year veteran Washington State Patrol trooper filed suit after colleagues allegedly created and circulated an AI-generated video depicting him in a sexually suggestive scenario designed to mock his sexual orientation. Likewise, a Nashville television meteorologist sued her former station after management failed to adequately address deepfake sexual images created using her likeness. And a Baltimore high school athletic director was sentenced to jail for creating a deepfake audio recording of his principal making racist and antisemitic comments.[1]

These aren't edge cases; They're the leading edge.

The Legal Framework

AI-generated content targeting an employee based on gender, race, sexual orientation, or other protected characteristics is analyzed under the same hostile work environment framework that governs traditional harassment claims under Title VII and analogous state laws. The technology is new. The legal exposure is

not.

Critically, **the employer does not need to have created the deepfake to face liability.** Courts will look at what the employer knew, when they knew it, and what steps they took to address the problem. Failing to act reasonably once the bad conduct comes to light is where employers get into trouble.

Beyond harassment and discrimination claims, employers may also face exposure under federal and state privacy statutes, defamation laws, and the growing patchwork of state legislation specifically targeting AI-generated deepfakes. States including California, Florida, Illinois, and Tennessee have enacted measures allowing victims to pursue both civil and criminal penalties. Federal legislation, including the DEFIANCE Act and the Take It Down Act, is advancing as well.

Why Your Handbook Needs Updating—Now

Most employer handbooks contain anti-harassment policies drafted before generative AI existed. Those policies tend to be high-level and generic. They reference "inappropriate conduct" or "offensive material" without addressing the specific risks posed by AI-generated content. That gap matters.

A policy that doesn't explicitly address AI misuse gives employees less notice and gives employers less cover. When litigation arrives—and it will—the strength of your written policies and the consistency of your enforcement will be among the first things examined.

Best Practices for Employers

1. **Update Anti-Harassment Policies to Address AI-Generated Content.** Your policy should explicitly prohibit the creation, distribution, or possession of AI-generated deepfake content that targets any individual based on protected characteristics, or that is otherwise harassing, defamatory, or sexually explicit. Don't rely on catch-all language. Name the technology, and leave no confusion as to your company's position.
2. **Implement a Standalone AI Acceptable Use Policy.** Consider a dedicated policy governing employee use of AI tools, both on company systems and personal devices, when the conduct affects the workplace. Define what's permitted, what's prohibited, and what the consequences are.
3. **Address Off-Duty Conduct.** Many deepfake incidents originate outside the workplace on personal devices, during off-hours. But when that content involves coworkers and circulates among staff, it becomes a workplace problem. Your policies should make clear that off-duty conduct creating a hostile work environment will be treated the same as on-duty misconduct. This is a common—and potentially catastrophic—employer misconception.
4. **Train Managers and Supervisors.** Managers need to understand that AI-generated harassment is real harassment. Train them to recognize it, report it, and escalate it. A manager who sees deepfake content

circulating and does nothing creates direct liability for the company.

5. **Establish Clear Reporting and Investigation Procedures.** Employees need a defined channel to report AI-generated harassment. Once a report is made, investigate promptly and document thoroughly. The adequacy of your response will be the central issue in any subsequent litigation.
6. **Enforce Consistently.** A policy that exists on paper but isn't enforced is worse than no policy at all. It demonstrates knowledge of the risk and a failure to act. Apply disciplinary measures uniformly, regardless of the employee's position or tenure.
7. **Monitor the Legislative Landscape.** State and federal deepfake legislation is evolving rapidly. What's compliant today may not be tomorrow. Work with counsel to ensure that your policies keep pace with the law.

The Bottom Line

AI deepfakes in the workplace aren't a theoretical risk. The lawsuits are already here. The technology is only getting better, cheaper, and more accessible. Employers who wait for a problem before updating their policies will find themselves defending the adequacy of those policies in front of a judge.

Review your handbook. Update your anti-harassment policies. Train your managers. The cost of prevention is a fraction of the cost of litigation.

If you have questions about updating your workplace policies to address AI-generated content, please contact Ryan O'Donnell (rodonnell@pullcom.com, (860) 424-4300), or any other attorney in Pullman & Comley's Labor, Employment Law & Employee Benefits practice group.

[1] Cases cited include *Pearson v. State of Washington, No. 25-2-14024-1 (Pierce Cty. Super. Ct. filed Dec. 19, 2025); Friedrichs v. Scripps Media, Inc., No. 3:25-cv-01494 (M.D. Tenn. filed Dec. 29, 2025);* **and** *State v. Darien, No. C-03-CR-24-002152 (Balt. City. Cir. Ct. 2024).*

Posted in Artificial Intelligence (AI)

Tags: Connecticut Employers, Employee Handbook, Employee Training