Lowenstein AI: A-I Didn't Know That
Video 10 – When AI Crosses the Line: Deepfakes, Harassment, and Employer Liability

By Bryan Sterba and Julie Levinson Werner

MAY 2026

Bryan Sterba: Welcome to another episode of "A-I Didn't Know That." Today I'm joined by my partner, Julie Werner, to discuss an issue at the intersection of AI and workplace harassment.

Julie, we're hearing more about artificial intelligence in the workplace, and one area that has drawn growing attention is the use of deepfakes and other realistic manipulated content. This is an issue that touches not only technology, but also employee relations, compliance, and legal risk, which means employers and HR teams really need to understand it.

So, why does this issue matter now, and what can or should employers be doing in response?

Julie Levinson Werner: Thanks, Bryan.

It's a really important topic because deepfakes are no longer just a theoretical concern or something that happens somewhere outside the workplace. These tools can create highly realistic images, videos, and audio, and when that content targets employees or circulates at work, it can create very serious legal and employee-relations issues.

Bryan Sterba: Let's start big picture: when people hear the term "deepfake," they may think of it as a tech issue or maybe just an online issue, but why has this become a real workplace issue for employers and HR professionals?

Julie Levinson Werner: It's a workplace issue because the harm doesn't stop with the technology itself. When deepfake content involving an employee is created or shared in the workplace, it can affect that employee's dignity, wellbeing, and ability to work.

The EEOC has already warned that sharing deepfake and other AI-generated images or videos at work can amount to harassing conduct based on legally protected characteristics. So, this is not just about misuse of technology, it can become a harassment, discrimination, and hostile work environment issue very quickly. And from an HR perspective, that means employers need to be

ready to respond to it the same way they would respond to other serious forms of workplace misconduct.

Bryan Sterba: What are the main risks for an employer? Are we mainly talking about harassment and hostile work environment concerns, or does the risk go beyond that?

Julie Levinson Werner: Harassment and hostile work environment claims are certainly front and center, but the risk can go beyond that. We've already seen employees sue employers based on allegations that deepfake content was created or circulated by coworkers and that the employer failed to respond appropriately.

What stands out in those cases is often that the claims focus not just on the existence of the deepfake, but also on what the employer did or did not do once it learned about the issue. Employees have alleged things like sexual harassment, sexual discrimination, hostile work environment, those are claims that are often alleged, but in addition, negligent retention, negligent supervision, retaliation, and failure to stop the dissemination of the content are also claims that are brought.

So, for employers, one of the biggest risks is not just that something happens, but that the organization fails to act quickly, seriously, and effectively once it becomes aware of the problem.

Bryan Sterba: How is the legal landscape evolving on this issue, and what should employers be paying attention to right now as they think about both federal and state developments?

Julie Levinson Werner: At the federal level, the Take It Down Act, a significant new framework that criminalizes the knowing publication of intimate visual depictions, including certain AI-generated digital forgeries, without consent.

There is also proposed federal legislation, what's called the DEFIANCE Act. The DEFIANCE Act would create civil remedies for victims and allow them to seek substantial damages, attorneys' fees, and in some circumstances proceed under pseudonyms.

At the state level, there are also laws targeting deepfakes, which adds another layer of complexity for employers who operate in multiple jurisdictions.

On top of that, there is still uncertainty because federal policy developments may affect how some state AI laws are treated going forward. So, for employers are dealing with an area where the law is developing quickly, this may remain unsettled for some time.

Bryan Sterba: So, from a practical standpoint, if an employer wants to be

proactive instead of reactive, what can they be doing?

Julie Levinson Werner: The first step is to make sure workplace policies are updated and clear. Employers can have policies that address the creation and distribution of deepfake content expressly and make clear that this kind of behavior can violate harassment and misconduct policies. It also may be grounds for discipline, including termination.

Training is also critical. HR professionals need to know how to respond to these complaints, and managers need to understand if they learn about an issue, they must elevate it immediately, rather than trying to handle it informally or dismiss it as a joke.

It's also important to have clear reporting and response protocols in place. Employers should think in advance about who needs to be involved when a complaint comes in, including HR, legal, and potentially IT, so the organization can move quickly and consistently.

Bryan Sterba: And if an employee reports that manipulated content involving them is being circulated, what should the employer's first response look like? What needs to happen right away?

Julie Levinson Werner: The first response should be prompt, serious, and supportive. The employee needs to know the complaint is being taken seriously, and the organization needs to move quickly to preserve evidence and understand what happened. That usually means documenting the complaint, preserving relevant materials, identifying where the content has been shared, and coordinating among HR, legal, and IT as appropriate.

If another employee may be responsible, the employer should promptly investigate, gather relevant evidence, interview the parties and witnesses, and take corrective action as warranted.

The employer also should think about employee support and practical containment. So for example, while HR may not be able to remove content from the internet on its own, employers can inform employees of their rights to seek removal under applicable law, and they also can work internally with IT to try to limit circulation on company systems or networks.

What employers should *not* do is minimize the complaint or delay action. In this area, inadequate response can become a major part of the legal risk.

Bryan Sterba: As employers think about AI more broadly, what is the key takeaway you would want HR professionals and business leaders to keep in mind when it comes to deepfakes in the workplace?

Julie Levinson Werner: Employers should treat this as a present day workplace risk, not a

future hypothetical. Deepfakes can create serious harm for employees and significant exposure for organizations, especially when employers are not prepared to respond. The best approach is for companies to be proactive: update policies, train the right people, establish reporting and response protocols, and stay informed about legal developments.

Ultimately, preparation, speed, and judgment are what matter most here.

Bryan Sterba: Julie, thank you so much for that thoughtful overview. Hopefully we were able to give employers a sense of both the legal risks and the practical steps organizations should be considering in this area.

We hope you'll all join us next time on "**A-I Didn't Know That**."