

Podcasts | June 23, 2026

# Fake Footage, Real Consequences: AI Deepfakes and Employment Risk

## SPEAKERS

[Tracey E. Diamond](#) | [Emily E. Schifter](#) | [Lawrence J. Cameron](#)

---

In this episode of *Hiring to Firing*, hosts [Tracey Diamond](#) and [Emily Schifter](#) examine the growing threat of AI deepfakes in the workplace through the lens of *The Morning Show*. Joined by [Lawrence Cameron](#), Troutman Pepper Locke partner in the firm's [White Collar Litigation + Investigations](#) group, they explore how AI-generated audio, video, and images can create new risks for employers, from fraud and disinformation to harassment, discrimination, and internal investigations. The conversation highlights the challenges employers face in determining what evidence is real, how deepfakes can complicate workplace misconduct investigations, and why companies should stay vigilant as the technology continues to evolve. Tune in for insights on how employers can prepare for deepfake-related incidents, respond appropriately when they arise, and better protect their workplaces in an era where seeing and hearing may no longer be believing.

Troutman Pepper Locke's [Labor + Employment Practice Group](#) provides comprehensive thought leadership through various channels. We regularly issue advisories that offer timely insights into the evolving employment law landscape, and maintain the [HiringToFiring.Law Blog](#), a resource spotlighting best practices for employers. Our [Hiring to Firing Podcast](#), hosted by Tracey Diamond and Emily Schifter, delves into pressing labor and employment law topics, drawing unique parallels from pop culture, hit shows, and movies.

## Transcript

### ***Hiring to Firing* — Fake Footage, Real Consequences: AI Deepfakes and Employment Risk**

**Hosts:** Tracey Diamond and Emily Schifter

**Guest:** Lawrence Cameron

**Recorded:** 6/3/26

**Aired:** 6/23/26

#### **Emily Schifter (00:00):**

Well, Tracey, today in our podcast episode, we are talking about AI deepfakes. And I feel like people see this a lot on social media, but we are seeing it more and more in the workplace. And one thing we didn't get a chance to dive into as much in our episode is kind of the opposite where somebody says that a video or picture of them is a deepfake and it turns out it's really not.

**Tracey Diamond (00:19):**

Yeah. A good example of that would be what I had heard about in the kiss cam incident was initially they said it must have been a deepfake because it wasn't them, and then they later on admitted that it was them. So that's just one example of many, I think we're going to see oftentimes in investigations where employees deny that they engaged in wrongful conduct, situations where they may now blame AI technology and say that it wasn't them, which creates even more issues from an investigation standpoint on determining what's real and what's fake. So listening to this episode, it's a fascinating and very frightening episode where we talk about the issue of deepfakes and their impact on the workplace.

[INTRO]

**Tracey Diamond (01:06):**

Welcome to *Hiring to Firing*, the podcast. I'm Tracey Diamond, a labor and employment partner with Troutman Pepper Locke, and I'm here with my co-host and partner, Emily Schifter. Together we tackle all employment issues from hiring to firing.

**Emily Schifter (01:19):**

Today, we're thrilled to have with us Lawrence Cameron, one of our partners in the White Collar practice group. Lawrence, thanks so much for joining us. We'd love to hear a little bit more about your practice and your background.

**Lawrence Cameron (01:30):**

Yeah, absolutely. Thank you all so much for having me. Really happy to be here. So I'm currently, as you said, a partner in our White Collar practice group. I joined the firm about a year ago after having most recently served as the acting US attorney in the US Attorney's Office for the Western District of North Carolina in Charlotte. So in that role, I oversaw all of the office's criminal investigations as well as our civil litigation. So that's everything from violent crime cases such as robberies and illegal gun possession to drug trafficking to complex fraud cases and cyber-involved offenses. So that's my background. And in terms of my current practice, building off that experience as a prosecutor, I represent companies in connection with internal investigations into allegations of all manner of wrongdoing. I also represent companies and individuals in connection with government investigations, including but not limited to criminal matters. And then finally, I leverage my trial experience to represent clients at trial in both civil and criminal cases.

**Emily Schifter (02:31):**

It's a fascinating background. I bet you have some amazing stories.

**Tracey Diamond (02:33):**

I was just thinking the same thing. Yeah. I would love to sit down with a cup of coffee and listen to all the stories.

Or a glass of wine, even better, and listen to all the stories, Lawrence. Well, we asked you today to talk about a topic that I think is really cutting-edge and fascinating and really, frankly, evolving, seems like in real time. Our topic for today is the issue of deepfakes and how it affects the workplace. As technology gets increasingly sophisticated, the possibility of fake content is so frightening. The possibility of fake content entering the workplace and causing a multitude of issues is getting more and more concerning. So, Lawrence, let's start with some definitions. What do we mean when we use this sort of fancy term, deepfake?

**Lawrence Cameron (03:14):**

At its simplest level, a deepfake is a video, audio, or image or set of images that are manipulated or generated by artificial intelligence to convincingly replace a person's likeness, face, or voice with another, or to make it appear that a person said or did something that they didn't say or do. So AI models are trained on vast amounts of data that includes images, audio, and so on and so forth of a specific person to learn their facial expressions, mannerisms, or vocal patterns, allowing the technology to map them onto a target person. So that's how a deepfake can be generated through the use of artificial intelligence.

**Emily Schifter (03:55):**

Tracey, I agreed. It's pretty terrifying that there could be a picture of you or a small clip of your voice and an AI model can just completely make it seem like you were somewhere you weren't or said something you didn't. Amazing the technology has come this far. So at the risk of stating the obvious, why might this be a concern? Why are we all so terrified?

**Lawrence Cameron (04:12):**

In terms of what I do, the biggest concern is the possibility of using this as a tool to commit fraud. So when you think about one of the classic fraud schemes, which is a business email compromise scheme, where a person sends an email impersonating the counterparty to a transaction and attempts to have that person wire them the funds instead of the true counterparty to that transaction. When you think about some of the guardrails that are put in place to prevent that from happening, such as pick up the phone and call the person to confirm that it is the actual counterparty to the transaction, when you think about how a deepfake can be used in a scheme like that, just as an example, when the person picks up the phone to call you to confirm that you're the counterparty, you can use this technology to imitate the likeness of the true individual on the other side of the line.

**Lawrence Cameron (04:57):**

So that's just one example of how this can be used to commit fraud. And you can think of, if you're creative enough, you can think of a lot of different ways that same sort of approach and technology can be used to commit all manners of fraud. But in a broader sense, disinformation. When you think about the different sources that we all receive our news and we all receive information from, the idea now that when someone sends you a link or sends you a story about something, you don't necessarily know whether it's true or whether it's a deepfake. And the result of that is it just causes mistrust. People can't tell what's real and what's fake anymore.

**Tracey Diamond (05:32):**

Are you seeing this fairly often in your practice now, Lawrence, or is it still sort of starting out?

**Lawrence Cameron (05:37):**

It's definitely still starting out, but we are seeing it. I recently spoke at a panel for mortgage fraud and people were sharing stories left and right about how they are seeing documents being generated through artificial intelligence, entire synthetic identities being created through artificial intelligence. And then as I stated about the business email compromise sort of example, that's not an example that I just made up. That is something that we're actually seeing in real life now.

**Tracey Diamond (06:06):**

Crazy stuff. So this would be a good time to introduce our first clip. Today we are revisiting the TV show *The Morning Show*, which stars Jennifer Aniston, Reese Witherspoon, and Billy Crudup. The show takes us behind the scenes at UBN, a fictitious TV network, as we see the plotting, the politics, and intrigue of TV news anchors and executives. We last spoke about this show, *The Morning Show*, back on our first season of Hiring to Firing, when we used the show's main plot about TV anchor Mitch Kessler, who is played by Steve Carell, to kick off a discussion about sexual harassment. Today we are focusing on season four, episode two, where Jennifer Aniston's character, Alex Levy, is falsely accused of plotting to assist an Iranian nuclear scientist to defect.

**Tracey Diamond (06:52):**

So let me back up for a minute because I think we need to provide some context for this first clip. Season four of *The Morning Show* opens with an AI version of Alex reporting on the Paris Olympics in dozens of languages all at once. We learn that this is a beta test of the use of AI to promote efficiencies and expand the network's reach, although there is grumbling amongst some of the employees that it may cost them their jobs, which is something I think we're hearing echoed across the workforce. Then Alex interviews Roya, an Olympic athlete from Iran. As they are setting up for the interview, Roya's father, whom Alex never met before, hands Alex a note that says, "We want to defect." Alex pulls Roya into the hallway to confirm this is really what she wants to do, and then acts quickly to pull the fire alarm so Roya and her father can make a rather dramatic exit.

**Tracey Diamond (07:42):**

What Alex didn't realize at the time is that Roya's father is a nuclear scientist, causing, as you can imagine, an international crisis. Alex is accused of colluding with the Iranians to facilitate the defection, and the network's executives show her CCTV footage of her conversation with Roya. Let's listen in.

[BEGIN CLIP]

**Celine (08:00):**

Good morning, Alex.

**Alex (08:02):**

Hey. John, right? From legal.

**John (08:05):**

Yes. Good to see you.

**Stella (08:07):**

Yeah. Alex, have a seat.

**Alex (08:11):**

Ooh, okay. Is this about Bradley?

**Stella (08:16):**

I'm going to ask you a question, and I need you to answer honestly, okay?

**Alex (08:21):**

Okay.

**Stella (08:25):**

The Iranian athlete and her father.

**Alex (08:28):**

Roya.

**John (08:28):**

Did you collude with the Naziris or their representatives to secure them asylum? Was the interview arranged for that purpose?

**Alex (08:35):**

Of course not. We went over this.

**Stella (08:40):**

And you didn't know that her father was a nuclear scientist, right?

**Alex (08:45):**

Not until you told me. I'm sorry, what is this?

**John (08:50):**

We've reviewed security footage in anticipation of any questions from the State Department. This is from our CCTV, and it picked up the audio.

**Alex (08:59):**

All right. So you got the layout that I sent? All right. My car's waiting downstairs, just like we planned. And believe me, believe me, your father's doing the right thing.

**John (09:07):**

Sounds premeditated. Apparently, you had talked to the girl about this before. What else did you promise her?

**Celine (09:11):**

Come on. Easy, John.

**Alex (09:12):**

That is... That's not what happened. It's not. I never met Roya before. I've never met her father.

**Stella (09:21):**

We can all hear it.

**Alex (09:22):**

I did not say that.

**Stella (09:23):**

Okay.

**Alex (09:24):**

I'm sorry. I don't know what the hell that is, but I did not say that. Okay? This is just crazy.

[END CLIP]

**Emily Schifter (09:31):**

Lawrence, getting back to the opening scene that Tracey described, where the company used an AI version of Alex to report on the Olympics in dozens of languages all at one time, what are your thoughts on the use of AI technology to enhance workplace efficiencies?

**Lawrence Cameron (09:45):**

Listen, I believe that AI is really a great tool to help with creating efficiencies, replacing menial tasks, or having the tools conduct or do these menial tasks instead of humans, creating efficiencies in recruiting and interviewing candidates, processing performance evaluations, monitoring workplace productivity, and so on and so forth. But there really are some significant risks with the use of generative AI. And I think the overall takeaway is that lack of trust if customers feel something's not authentic is a really significant risk, as is the potential inability to control what the technology does or says. And then certainly, as we just heard from the clip, the issue of deepfakes is another one of those risks.

**Emily Schifter (10:30):**

Definitely. And not to mention all of the various state laws that are now coming out for employers who want to use this for things like recruiting or hiring or evaluating, which is a whole 'nother topic, could be its own podcast. But getting back to the issue of deepfakes, so as we will hear in our next clip, Alex is completely frustrated that someone could manipulate her voice in this way and that no one believes her when she says she's telling the truth. So let's listen in.

[BEGIN CLIP]

**Cory (10:54):**

You want to talk about it?

**Alex (10:56):**

I'd love to talk about it.

**Cory (10:56):**

All right. Let's talk.

**Alex (10:58):**

I just can't talk about it.

**Cory (11:00):**

Okay.

**Alex (11:01):**

Can't legally talk about it. So... All right. You know what? I've been... I've been deepfaked. Okay? There it is. I said it. There is audio of me saying something that I did not say. But I can't prove that I didn't say it. And if I did say it, it would be so, so bad if I did. And absolutely no one believes me. Stella, Celine, none of them believe me. I can't prove it. It's not real. And I'm kind of losing my mind.

**Cory (11:33):**

You're being gaslit.

**Alex (11:36):**

Yes. That's what it is.

[END CLIP]

**Tracey Diamond (11:40):**

So, Emily, I now have a question for you. Have you heard about any cases involving the use of deepfake technology?

**Emily Schifter (11:47):**

So in the employment context, unfortunately, as you would suspect, we mostly see this coming up in a sexual harassment kind of a context, people manipulating images or chats in a pornographic manner. So a couple of recent examples that we dug up: a California appellate court recently affirmed a jury verdict awarding \$4 million to a police captain who was subjected to a hostile work environment after a sexually explicit AI-generated image resembling her was widely circulated in the workplace. And there, the court found that the dissemination of that fabricated content constituted unlawful harassment under California law.

**Emily Schifter (12:24):**

Another case, also involving police, a Washington state trooper filed suit alleging that a supervisor used AI to create and circulate a deepfake video of him intimately kissing a coworker. The officer is now suing his employer for discrimination, retaliation, and invasion of privacy. And this is something that courts and agencies have recognized could be harassment. Prior to rescinding its prior harassment guidance, the EEOC, for example, had specifically called out concerns with deepfake technology. And the prior guidance explicitly stated that the sharing of pornography or sexually demeaning depictions of people, including AI-generated and deepfake images and videos, was an example of harassment and violation of Title VII. So just kind of confirming that just because it's AI, just because a machine generated it, doesn't mean that it can't still be harassment.

**Tracey Diamond (13:15):**

There's somebody behind the machine, right? The Wizard of Oz pulling the levers.

**Emily Schifter (13:18):**

Exactly.

**Tracey Diamond (13:19):**

So certainly the use of deepfakes to create images of coworkers engaging in sex acts is an issue, obviously. This was also illustrated in *The Morning Show* episode where Alex's coworker suggests that she Google her name and the term deepfake. And when she does, she finds many links to pornographic sites using her name and image. But can deepfakes create issues in the workplace beyond sexual harassment? What do you think, Lawrence?

**Lawrence Cameron (13:44):**

Absolutely. In the first instance, I'll note that when I was at the US Attorney's Office, we actually prosecuted an individual for child sexual abuse materials related offenses based on the manipulation of images using deepfake technology. And also I previously mentioned the sort of business email compromise scheme, manner in which someone could use deepfake technology to commit a crime. So the bottom line is if AI can be used to make it seem like someone said something they didn't or is pictured in a way that they weren't in fact photographed or videoed, that's a problem. You can imagine all sorts of improprieties or errors that can result from that kind of a circumstance. From a discrimination perspective, it could be used to mock workers by changing their skin tone or ethnic features as an example, or making it appear as though someone has a disability when they do not.

**Emily Schifter (14:33):**

I think that's right. And it sounds like there could be a criminal component to liability, kind of similar to the discrimination context. Just because AI doesn't mean that you aren't going to be liable. Is that right, Lawrence?

**Lawrence Cameron (14:44):**

That's correct. If someone uses AI to commit a crime, then that's just as much of a crime as though it was committed without the use of AI, right? So if someone uses AI to interfere with business or steal something that doesn't belong to them or to commit another crime, that's just as much a crime as if they'd done it personally. And then there's also charges related to cyber harassment, violation of obscenity laws, non-consensual pornography under federal or state laws are also possible. And then there's also the issue of potential violation of state privacy laws, which, as you stated earlier, could be its own podcast episode.

**Emily Schifter (15:16):**

That's right. So what about with regard to investigations? In *The Morning Show* episode, the network was convinced that Alex had colluded with the Iranians based on the altered CCTV footage. Does the possibility of deepfakes create challenges in investigating workplace misconduct?

**Lawrence Cameron (15:32):**

It absolutely could. Because if you don't know whether you can rely on evidence that you've gathered, whether it's surveillance footage, cell phone or instant messages, photographs or emails, then that really undercuts the core process and approach for conducting investigations. How can you rely on the findings if you can't rely on the underlying evidence that's been gathered?

**Tracey Diamond (15:51):**

And that kind of leads me to a question that's been on my mind since we started talking about this in this episode, which is that even though the technology is getting more and more sophisticated, are there ways to tell what's real from what's fake? Can we get around this and get to the truth here?

**Lawrence Cameron (16:06):**

There are a number of indicators. Again, we should put a timestamp on this, right? June 3, 2026, given the current state of technology. Certain indicators of a deepfake include unnatural blinking, mismatched lighting, glitches around the face or the mouth, and robotic audio. But as the technology continues to improve quite rapidly, it is getting harder and harder to distinguish between what is real and what is fake. So I think general awareness, just knowing that this is a possibility. And so to be on the lookout for things that don't add up and staying vigilant are really critical, just as you would for malicious emails or spam phone calls.

**Tracey Diamond (16:44):**

Maybe something that employers should consider adding to their training on electronic communication systems in general is the kind of things to be looking out for to tell what's real from what's fake.

**Lawrence Cameron (16:54):**

That's exactly right.

**Emily Schifter (16:55):**

So we've talked about some of the existing laws that might apply to conduct that people use AI deepfakes to engage in, but are there any laws that have been passed that specifically address or try to combat this issue, Lawrence?

**Lawrence Cameron (17:07):**

Yeah. So at the federal level, there was a significant law passed in 2025, and that's the Federal Take It Down Act. So this is significant for a number of reasons. First, it makes non-consensual intimate images, including AI deepfakes, a federal crime. So if you share someone's intimate image without their consent, you can be charged under this new federal law, whether it's, one, a real photo or video, or an edited image, or an AI-generated deepfake. Threatening to post such an image or video also counts. Second, platforms really have to move fast.

Once a victim reports a non-consensual intimate image under this law, platforms have 48 hours to take it down. That's crucial for AI deepfakes, which can spread and multiply quickly.

**Lawrence Cameron (17:51):**

And so under this law, the burden shifts from the victim checking platforms to the platforms being legally on the clock once they're put on notice. And then third, it protects people who report in good faith. So if you report one of these images, especially if it targets you, you're protected from being sued just for trying to get it removed. That's meant to make it safer to speak up, whether the content is a leaked photo or a hyper-realistic AI deepfake.

**Tracey Diamond (18:16):**

What about Florida? I understand there's a good example under Florida law.

**Lawrence Cameron (18:19):**

Yeah, that's right. So I just talked about a federal law, but the states are taking action too. Florida's Brooks Law is a really good example of what some states are doing to address this issue. It requires websites and online services to quickly remove sexual deepfakes and other altered sexual images, plus any copies within 48 hours after the victim asks. It also forces platforms to set up a reporting process, gives them some legal protection if they act in good faith, and penalizes them under Florida's consumer protection laws if they don't comply.

**Tracey Diamond (18:48):**

Okay. If an employer discovers that a deepfake incident has occurred in their workplace, a coworker created an inappropriate clip of a colleague, what should be their first steps to respond?

**Emily Schifter (18:59):**

I think this is such a good question because I have had clients in this situation, and because of the AI angle, they feel like, "Oh my gosh, what do we do? This is so new and novel, and how do we handle it?" But I think it's kind of as we've been discussing. You treat it like any other incident of harassment or discrimination. You have to investigate, obviously take remedial action as needed, consistent with your policies, like you would for any other incident. And of course, there are confusing pieces to it. I had one situation where there was an allegation and the accused actually said, "This image is not real of me," kind of similar to Alex in our Morning Show clip. And the employer was stuck trying to figure out, "Is this real? Is this fake?" and kind of the challenges you mentioned, Lawrence, of you've got evidence, but what can you trust? So that does add a layer of complexity, to be sure. But treating it like any other investigation where you're weighing evidence and determining credibility of witnesses, making sure that you're again taking remedial action where needed, super important.

**Tracey Diamond (19:52):**

Are there any other recommended next steps, Lawrence?

**Lawrence Cameron (19:54):**

I would say depending on the particular facts and circumstances, you may want to consider reporting the incident to law enforcement, particularly in light of some of the consumer protection laws we've mentioned. Another step would be if you're an employer facing a circumstance such as what was just described, you really strongly consider reaching out to counsel to seek guidance on next steps. The last thing you want to do is try to mitigate a potential circumstance in your employment while running afoul of one of these various state consumer protection laws without necessarily knowing that you're doing so.

**Emily Schifter (20:24):**

That certainly makes a lot of sense. And that brings us to our last clip. In this last clip, Alex is seen anchoring a Morning Show segment on climate change and gives a word of warning to her audience about the danger of the use of AI technology.

[BEGIN CLIP]

**Alex (20:38):**

In a world of deepfakes, conspiracies, and corporate propaganda machines, we have to question everything that we see and we hear now more than ever. And that's what these protesters were doing.

**Yanko (20:50):**

Look, I'm just going to say this, and you both know me, I've been shouting about climate change for years now, but I mean, come on, Alex. Stopping traffic and vandalizing property, that can't be the answer, right?

**Alex (20:59):**

Understood. But when no one is taking real action, is breaking the law justifiable for the greater good?

**Yanko (21:05):**

So, the ends justify the means? Let's take a look at what happened yesterday, okay? And look, I see what you mean. It's a complicated situation.

[END CLIP]

**Emily Schifter (21:13):**

Certainly a timely warning for all of us. So thank you so much for joining us today, Lawrence.

**Lawrence Cameron (21:18):**

Thank y'all for having me.

**Emily Schifter (21:19):**

Thank you so much as always to our audience for listening in. Don't forget to visit our blog, [HiringToFiring.Law](#), and subscribe so you can get the latest updates. Please make sure that you also subscribe to this podcast on whatever podcast platform that you like to use, and we look forward to next time.

---

*Copyright, Troutman Pepper Locke LLP. These recorded materials are designed for educational purposes only. This podcast is not legal advice and does not create an attorney-client relationship. The views and opinions expressed in this podcast are solely those of the individual participants. Troutman does not make any representations or warranties, express or implied, regarding the contents of this podcast. Information on previous case results does not guarantee a similar future result. Users of this podcast may save and use the podcast only for personal or other non-commercial, educational purposes. No other use, including, without limitation, reproduction, retransmission or editing of this podcast may be made without the prior written permission of Troutman Pepper Locke. If you have any questions, please contact us at [troutman.com](#).*

---

*DISCLAIMER: This transcript was generated using artificial intelligence technology and may contain inaccuracies or errors. The transcript is provided "as is," with no warranty as to the accuracy or reliability. Please listen to the podcast for complete and accurate content. You may [contact us](#) to ask questions or to provide feedback if you believe that something is inaccurately transcribed.*

**RELATED INDUSTRIES + PRACTICES**

- [Labor + Employment](#)
- [White Collar Litigation + Investigations](#)