Insights, News & Events

YOU CAN NO LONGER BELIEVE WHAT YOU SEE: 5 WAYS EMPLOYERS CAN GUARD AGAINST DEEPFAKES

Insights
Nov 9, 2023

In their book, "AI 2041: Ten Visions for Our Future," Kai-Fu Lee and Chen Qiufan point out that we used to live in a world where we could trust video evidence, but not anymore. Thanks to deepfakes – sophisticated digital forgeries that use artificial intelligence to manipulate or generate audio and visual content with a high degree of realism – we now live in a world where we all need to adjust our thinking when it comes to video and audio recordings. Employers are not immune from this changing environment and will need to take active steps to address what is sure to be a growing problem in the near future. What are the five ways employers can guard against deepfakes?

What are Deepfakes?

At their essence, deepfakes are really, really good imitations. They are videos, audio, photos, text messages, and other forms of media created using AI that are extremely hard to differentiate from the real or authentic thing. The intention of deepfakes is to convince someone that something happened when it did not actually occur.

Deepfakes already play a prominent role in our culture. In 2018, Jordan Peele created a deepfake video of former President Obama badmouthing a political rival, and the next year a prominent YouTube artist seamlessly morphed Tom Cruise's face onto Bill Hader's to make it appear as if Hader's impression of the actor had taken on real life.

But the times are already drastically changing and these videos seem quaint compared to what now exists – and

Related People

Karen L. Odash

Associate

610.230.2165

David J. Walton, AIGP, CIPP/US

Partner

610.230.6105

what's soon in store. Thanks to incredible advances in AI, the entire world has access to programs and apps that allow you to create and transform images, video, and recordings in incredibly realistic ways. Despite the complicated process that takes place behind the scenes, the software used to make deepfakes is now readily accessible to all. A recent report indicated that advanced deepfake technology that makes it virtually impossible for people to distinguish fake videos from real will be available to everyone – even beginners – by next year.

What makes today's deepfakes different than those of just a few years ago? Since deepfake artists use deep learning AI to replace the imagery and improve their product, the explosion in generative AI technology and the access to highly powerful modeling systems now at all of our fingertips means that deepfakes in 2023 are more convincing than ever. And no doubt 2024's deepfakes will be even more realistic.

Deepfakes Are Already Causing Major Societal Concerns

Not surprisingly, deepfake creators aren't just making amusing and entertaining videos – they are being used for more nefarious means.

Earlier this year, a group of students in NY made a deepfake recording of their principal making racist remarks and threatening students, which caused a firestorm of controversy when it circulated among the school community. Just last month, high school students in New Jersey were caught making deepfake nude images of fellow students and sharing these images by group texts. In fact, Wired reported that 54% more deepfake pornographic videos were uploaded to websites in the first nine months of 2023 than in all the previous year.

But the deepfake controversy goes well beyond problems among teens and at schools. We have seen allegations in court that parties are submitting fake evidence using deepfakes, political parties and candidates creating fake videos depicting their rivals or problems that might befall society should their rival win an election, forged speeches from government officials making controversial statements to the general public, and allegations that wartime footage has actually been digitally manipulated.

Service Focus

AI, Data, and Analytics

Resource Hubs

AI Governance Hub

In June, in fact, the FBI released a public service announcement warning of malicious actors "manipulating benign photographs or videos" to create deepfakes and target victims. This warning is an acknowledgment that deepfakes can meticulously craft an illusion designed to destroy a career and reputation, and we must all come to terms with this reality and understand that we can no longer automatically trust what we see with our own eyes.

Why Should Employers be Concerned About Deepfakes?

Any problem impacting society as a whole usually impacts the workplace, and deepfakes are no exception. Some ways that deepfakes are already hitting the workplace:

- Based on the nefarious uses of deepfakes described above, it's not hard to see how this technology could be used to create offensive content at the workplace. We will soon see cases involving fake videos or audio recordings of workers doing something offensive or otherwise improper. Deepfakes relied upon during internal investigations could lead to wrongful disciplinary actions or terminations.
- In June 2022, the FBI issued a warning that deepfakes were being used in remote job interviews, a tool that gained steam during the height of the pandemic and which remains a continued mechanism for initial interviewing.
- And of course, deepfakes can easily mimic the voices – and videos – of top executives to help hackers steal money from your company, taking the established text/email scam to the next level.

5 Considerations to Mitigate the Risk of Deepfakes

To guard against deepfakes, employers can take several proactive measures:

1. **Offer Your Workers Deepfake Training:** Employers should educate themselves and their employees about the existence and potential dangers of deepfakes. This includes understanding how they work, their potential impact on the organization, and the importance of staying vigilant. This must involve fostering a culture of skepticism, similar to the way that employees are now on guard for phishing emails. Employers should have a

critical mindset when consuming media, particularly when it comes to verifying the authenticity of audio, video, or written content. Provide training to workers about some ways to spot deepfakes (looking for blurry details, irregular lighting, unnatural eye or facial movements, mismatched audio, absence of emotion, etc.). As part of overall training, make sure your cybersecurity training is up to date and required for all employees.

2. **Develop Channels for Open Communication**: Employees must feel comfortable questioning the legitimacy of information and reporting any suspicious activity. Encourage employees to speak up. You should promote a culture where employees are comfortable questioning the legitimacy of information and reporting any suspicious activity. Give employee examples of requests that are abnormal or outside the normal company procedures. Employees should never be afraid of speaking up about these issues.

3. **Make Sure IT Adopts Robust Authentication Protocols:** Employers should establish strong authentication measures for access to sensitive information, systems, and accounts. This may include multi-factor authentication, biometric verification, or other secure methods to minimize the risk of unauthorized access. Also, there must be failsafe measures for the requests involving financial and security issues. Assume that nefarious actors will use deepfakes to try to steal from your company.

4. **Invest in New Threat-Detection Tools:** This is a developing area. Technology to protect against deepfakes has not kept up with the overall deepfake technology. But stay up to speed in this area and look for opportunities to invest in advanced technologies such as AI-powered deepfake detection tools as they become more robust, as they will help identify and flag potential deepfakes.

5. **Review Your Policies**: Make sure your policies prohibit your employees from creating deepfakes involving company personnel and company proprietary information. There are very few legitimate businesses uses for most companies. In general, employees should not be allowed to use employer resources or data to create deepfakes.

Conclusion

If you have questions, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our Artificial Intelligence Practice Group. Make sure you subscribe to Fisher Phillips' Insight System to gather the most up-to-date information on AI and the workplace.