

The

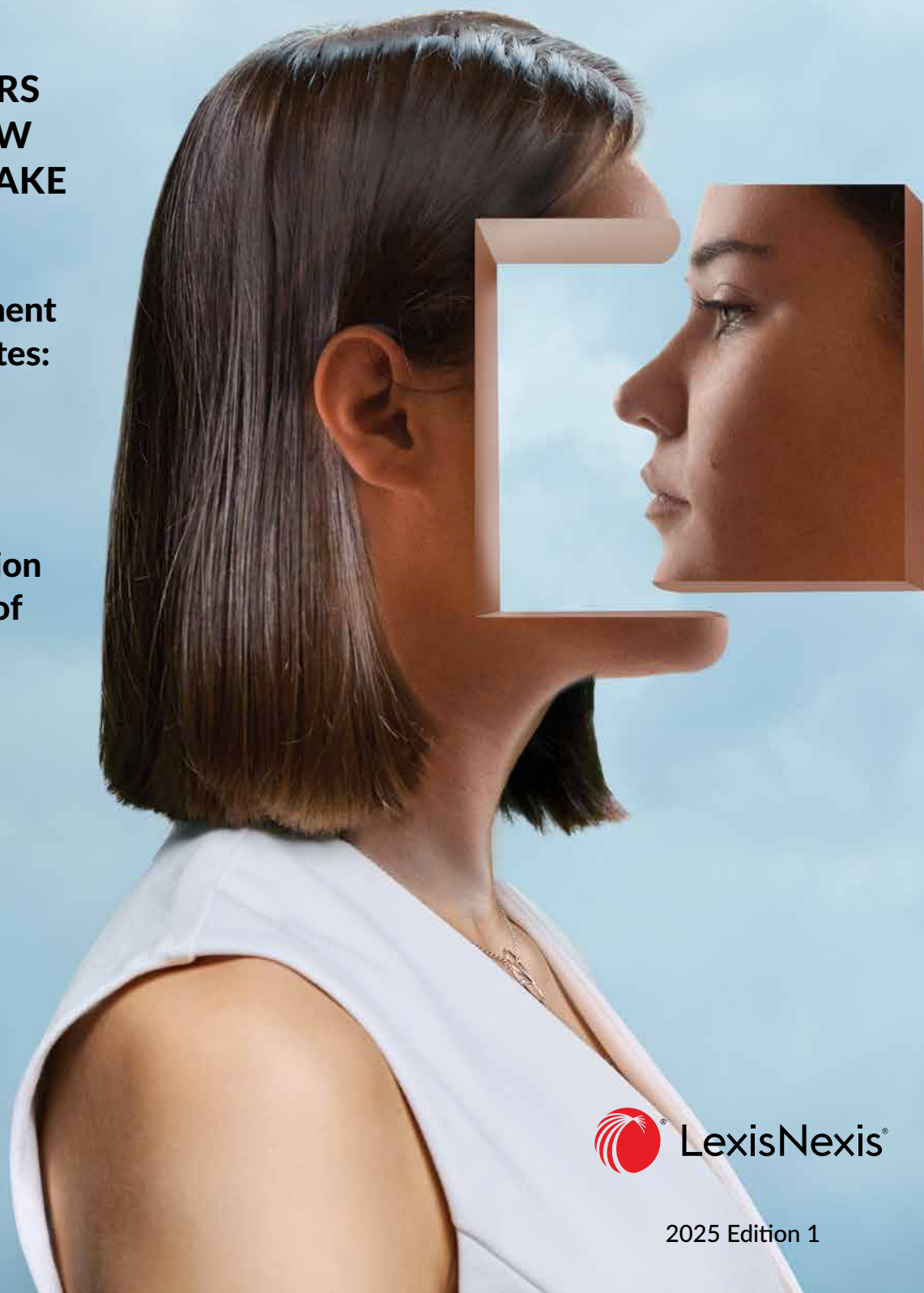


PRACTICAL GUIDANCE Journal

WHAT LAWYERS NEED TO KNOW ABOUT DEEPFAKE TECHNOLOGY

**AI Risk Management
in the United States:
Looking Ahead**

**Examining the
Application of
Anti-Discrimination
Laws to the Use of
AI Technology**



LexisNexis®

2025 Edition 1

Welcome to what comes next.

Lexis+ AI returns trusted results backed by verifiable authority 2X faster than Westlaw®, enabling you to work more efficiently than ever.

Transform your legal work

LEARN MORE: [LEXISNEXIS.COM/AI](https://www.lexisnexis.com/ai)

Current Legal Developments

4 WHAT LAWYERS NEED TO KNOW ABOUT DEEPFAKE TECHNOLOGY

Civil Litigation

12 AI RISK MANAGEMENT IN THE UNITED STATES: LOOKING AHEAD

Data Security & Privacy

Practice Notes

20 KEY AI LEGAL ISSUES IN DEI & EMPLOYMENT DISCRIMINATION

Labor & Employment

32 EXAMINING THE APPLICATION OF ANTI-DISCRIMINATION LAWS TO THE USE OF AI TECHNOLOGY

Labor & Employment

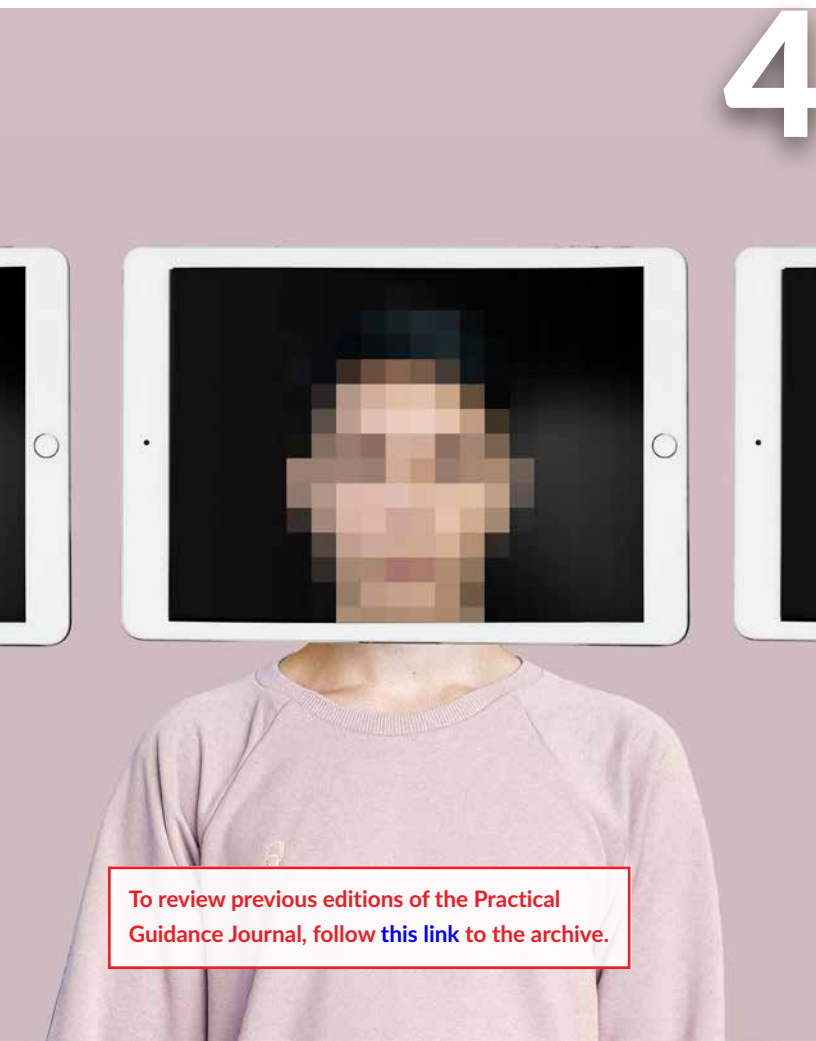
Practice Tips

38 ARTIFICIAL INTELLIGENCE AGREEMENTS CHECKLIST

Intellectual Property & Technology

Rule of Law

46 INNOCENCE CANADA SEEKS JUSTICE FOR WRONGLY CONVICTED



To review previous editions of the Practical Guidance Journal, follow [this link](#) to the archive.



MANAGING EDITOR	Lori Sieron
DESIGNER	Jennifer Shadbolt
CONTRIBUTING EDITORS	
Bankruptcy	Mark Haut
Capital Markets	Victor Cohen
Civil Litigation	Randi-Lynn Smallheer
Construction	Kimberly Seib
Commercial Transactions	Esther Kim
Data Security and Privacy	Barbara Reece
Employee Benefits & Executive Compensation	Rex Iacurci
Finance	Sherry Mitchell
Financial Services Regulation	Celeste Mitchell-Byars
Insurance	Karen Yotis
Healthcare	Rodney Miller
Intellectual Property & Technology	Miri Beiler
Labor & Employment	Elias Kahn
Life Sciences	Jason Brocks
Energy & Utilities	Cameron Kinvig
Real Estate	Sara Kolb
Tax	Rex Iacurci
ASSOCIATE EDITORS	Maureen McGuire
	Mia Smith
	Shannon Weiner
	Ted Zwayer
WEBSITE MARKETING & DESIGN	Sherica Apo
	Alainna Nichols



The Practical Guidance Journal (Pub No. 02380; ISBN: 978-1-6328t-895-6) is a complimentary resource published quarterly for Practical Guidance subscribers by LexisNexis, 230 Park Avenue, 7th Floor, New York, NY 10169. | Website: www.lexisnexis.com/PracticalGuidance-Product

This publication may not be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form, in whole or in part, without prior written consent of LexisNexis. Reproduction in any form by anyone of the material contained herein without the permission of LexisNexis is prohibited. Permission requests should be sent to: permissions@lexisnexis.com.

All information provided in this document is general in nature and is provided for educational purposes only. It may not reflect all recent legal developments and may not apply to the specific facts and circumstances of individual cases. It should not be construed as legal advice. For legal advice applicable to the facts of your particular situation, you should obtain the services of a qualified attorney licensed to practice in your state.

The publisher, its editors and contributors accept no responsibility or liability for any claims, losses or damages that might result from use of information contained in this publication. The views expressed in this publication by any contributor are not necessarily those of the publisher.

Send correspondence to: The Practical Guidance Journal, 230 Park Avenue, 7th Floor, New York, NY 10169. Periodical Postage Paid at New York, New York, and additional mailing offices.

LexisNexis and the Knowledge Burst logo are registered trademarks. Other products and services may be trademarks or registered trademarks of their respective companies.

Copyright 2025 LexisNexis. All rights reserved. No copyright is claimed as to any part of the original work prepared by a government officer or employee as part of that person's official duties.

Images used under license from istockphoto.com.

EDITORIAL ADVISORY BOARD

Distinguished Editorial Advisory Board Members for The Practical Guidance Journal are seasoned practitioners with extensive background in the legal practice areas included in Practical Guidance. Many are attorney authors who regularly provide their expertise to Practical Guidance online and have agreed to offer insight and guidance for The Practical Guidance Journal. Their collective knowledge comes together to keep you informed of current legal developments and ahead of the game when facing emerging issues impacting your practice.

Andrew Bettwy, Partner
Proskauer Rose LLP
Finance, Corporate

Julie M. Capell, Partner
Davis Wright Tremaine LLP
Labor & Employment

Candice Choh, Partner
Gibson Dunn & Crutcher LLP
Corporate Transactions,
Mergers & Acquisitions

**S. H. Spencer Compton,
Sr. VP and Sr. Counsel**
Commonwealth Land Title
Insurance Co.
Real Estate

Linda L. Curtis, Partner
Gibson, Dunn & Crutcher LLP
Global Finance

**Tyler B. Dempsey,
General Counsel**
REPAY

James G. Gatto, Partner
Sheppard, Mullin, Richter &
Hampton LLP
Intellectual Property, Technology

Ira Herman, Partner
Blank Rome LLP
Insolvency and Commercial Litigation

Ethan Horwitz, Partner
Carlton Fields Jorden Burt
Intellectual Property

Glen Lim, Partner
Katten Muchin Rosenman LLP
Commercial Finance

Joseph M. Marger, Partner
Reed Smith LLP
Real Estate

Matthew Merkle, Partner
Kirkland & Ellis International LLP
Capital Markets

Timothy Murray, Partner
Murray, Hogue & Lannis
Business Transactions

Michael R. Overly, Partner
Foley & Lardner
Intellectual Property, Technology

Leah S. Robinson, Partner
Mayer Brown LLP
State and Local Tax

Meredith French Reedy, Partner
Moore & Van Allen PLLC
Financial Services

Scott L. Semer, Partner
Torys LLP
Tax, Mergers and Acquisitions

**Lawrence Weinstein,
Sr. Counsel, Technology
Transactions**
ADP

Kristin C. Wigness, Sr. Counsel
McGuireWoods LLP, Finance,
Restructuring & Insolvency

Patrick J. Yingling, Partner
King & Spalding
Global Finance

Introduction

2025 WILL NO DOUBT CONTINUE THE accelerated use of artificial intelligence (AI) technology and advancements that allow the legal world to increase efficiency and create time and resource savings. On the side of caution and concern, attorneys and firms are forced to prepare for the darker side of AI capabilities, deepfakes and fraudulently manipulated media and data. In this edition of The Practical Guidance

Journal, we present guidance on detecting deepfakes and strategies for spotting fake evidence as the use of reality-altering technologies escalates.

More cautionary AI guidance is included in the forward-looking article on AI risk management. In the current atmosphere of patchwork AI regulations developed across federal agencies, this article sets out to

clarify AI risk management techniques for legal and business professionals.

Also in this edition is a checklist of key legal considerations for attorneys advising clients when drafting contracts involving AI. For employers, review the articles offering insights on using AI in hiring and avoiding potential discrimination issues. We also provide a summary of featured content recently added to Practical Guidance.

Our mission

The Practical Guidance Journal is designed to help attorneys start on point. This supplement to our online practical guidance resource, Practical Guidance, brings you a sophisticated collection of practice insights, trends, and forward-thinking articles. Grounded in the real-world experience of our 2000+ seasoned attorney authors, The Practical Guidance Journal offers fresh, contemporary perspectives and compelling insights on matters impacting your practice.



Bijan Ghom SAXTON & STUMP

What Lawyers Need to Know about Deepfake Technology



This article addresses existing deepfake technology and covers topics such as the available platforms to both create and detect deepfakes and the best practices for dealing with deepfakes in your case.

A DEEPPFAKE IS MANIPULATED MEDIA THAT CONVINCINGLY mimics real people and real events. While you may not have dealt with a deepfake in your practice, you likely have dealt with a forgery or falsified evidence of some kind. Some of the practices and strategies that apply to fighting fake evidence generally apply to deepfakes. That said, sticking to your old habits might not be enough to keep a deepfake from the jury and may even prevent you from spotting the deepfake until it is too late. Deepfakes are master forgeries—expertly crafted fabrications that are so good they can be impossible for the human eye and ear to distinguish them from genuine evidence. We are just scratching the deepfake surface as companies are aggressively improving these reality-altering technologies.

Deepfake Creation Tools

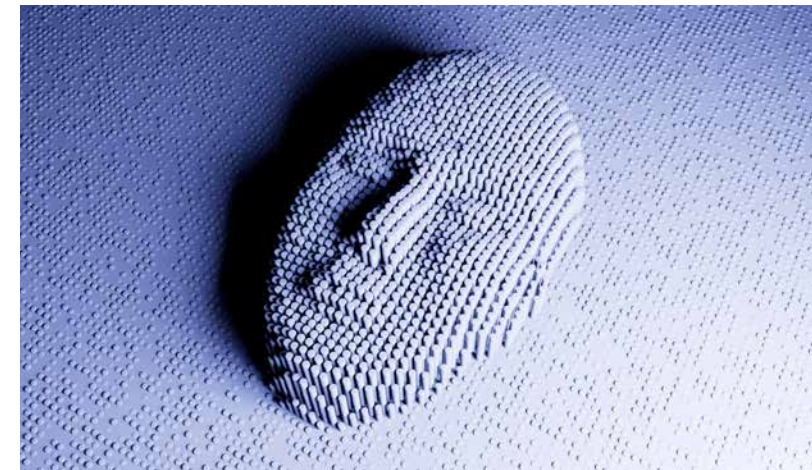
While deepfake is not a technical term, it typically refers to images, videos, or audio that are edited or manufactured using artificial intelligence—and usually the term refers to images, video, or audio of real people. Hence the danger. Although you may have dealt with fake evidence before, such as a forged document or even a lying witness, a deepfake has an advantage: it is created by an AI model that is trained for the very purpose of deceiving the human eye. In fact, and as discussed below, the AI model goes through internal rounds of testing to make sure it is realistic enough to deceive you, and it will even restart the process if it is not.

You should start familiarizing yourself with some of the names of the technology platforms that are used to create deepfakes in the same way that you are now familiar with apps like Snapchat and WhatsApp. You may come across a file extension, an email, or even see one of these applications in a party's browser history or on the list of the applications stored on the phone of a key witness. You should have a basic understanding of the underlying technology to know what to look for.

Videos and Images

Probably the most feared deepfake evidence is a video. Videos have tremendous influence in the courtroom. Even one piece of video evidence can be disastrous for litigants.¹

Videos have an immediate impact on the jury and illustrate events in a more powerful way than oral testimony.² During deliberation, videos and images greatly enhance the juror's ability to recall events.³

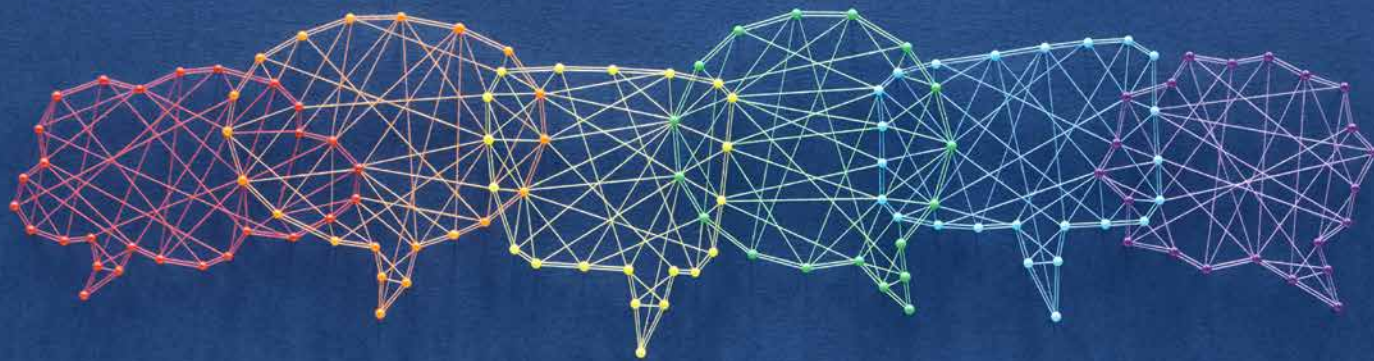


Below is a list of several of the more well-known and sophisticated platforms in the deepfake world:

- Synthesia⁴ offers an AI video-creation platform that enables users to generate synthetic videos using avatars. The company seems to focus on corporate training and marketing videos. A deepfake video can be created by entering a simple text prompt. Note that DeepBrain AI and Rephase.ai are two similar platforms and both focus on video-creation corporate and marketing use.
- Zao⁵ is a popular Chinese application that allows users to swap faces in videos and pictures. Unlike Synthesia, Zao focuses more on user-generated content for personal or entertainment use.
- DeepFaceLab⁶ is an open-source tool that is available for free to anyone who wants to create a deepfake video. Whereas Zao is made to be user-friendly and fun, DeepFaceLab is said to be the most realistic face-swapping video tool available. It is marketed to developers, and developers are free to use the code to create their own versions and train their models with few restrictions.
- FaceApp⁷ is a popular application known for its filters and transformations to existing videos or images. Although FaceApp does not create deepfakes like the other platforms discussed, it can enhance or alter images and videos. While FaceApp is known most for its ability to modify lighting or fix imperfections in a video, it can also change the hair color, age, or gender of a person.

¹ See *Scott v. Harris*, 550 U.S. 372, 378–81 (2007), finding summary judgment should be granted when a video shows the plaintiff's "version of events is so utterly discredited by the [video evidence] that no reasonable jury could have believed him." ² *United States v. Watson*, 483 F.3d 828 (D.C. 2007). ³ See Karen Martin Campbell, *Roll Tape—Admissibility of Videotape Evidence in the Courtroom*, 26 U. Mem. L. Rev. 1445, 1447 (1996). Studies show that jurors are 650% more likely to retain information when they hear oral testimony coupled with video testimony than those who only hear oral testimony. ⁴ About Synthesia - Read our story here. ⁵ Download ZAO. ⁶ DeepFaceLab 2.0. ⁷ About Us - FaceApp.

Understanding the basic mechanics underlying deepfake technology is the first step to defending against them. Like any scientific or specialized area, a basic understanding of the landscape will allow you to ask the right questions....



■ Avatarify⁸ allows users to create a live impersonation of a person with just an image of that individual. Avatarify may be integrated with popular video-conferencing platforms, and thus has the potential to be used for deception in remote court proceedings like virtual hearings.

Audio

Below are some platforms for making deepfake audios:

■ Descript (including Lyrebird)⁹ and Resemble AI¹⁰ are two different platforms that offer voice cloning to generate synthetic audio of the original speaker. Only a few minutes of audio is needed for

these platforms, and the synthetic audio can be generated by inputting text of the desired audio.

■ VoiceAI¹¹ is a modulation tool that can alter voices in real time for free. VoiceAI can modify live audio streams. This is a powerful tool for impersonation and a concern for virtual hearings, depositions, and even remote testimony at trial.

These products are frequently marketed as easy to use, with no skills or training required. You thus have to be on guard for the use of such applications in your cases, including situations where your own clients may offer up deepfakes.

8. Avatarify - Bring your photos to life. 9. About Descript. 10. Resemble AI - The All-in-One AI Voice Platform. 11. We're Building the Future of Voice Technology - Voice.ai.

Deepfake Detection Tools

Understanding the basic mechanics underlying deepfake technology is the first step to defending against them. Like any scientific or specialized area, a basic understanding of the landscape will allow you to ask the right questions of the parties, witnesses, and experts, and then use the responsive information favorably.

The deepfake process has generally five steps:

1. **Data collection.** The user inputs media (images, videos, or audio) of the target person whose face or voice will be synthesized.
2. **Data processing.** Some of the collected data is then analyzed using algorithms to identify key features such as facial structures, movements, and voice patterns. Often, a portion of the data is reserved for the model training process so the model can be checked against unseen data of the same person.
3. **Model training.** The machine learning model is then trained on the input data and learns to generate new images or audio by comparing its outputs with the unseen data.
4. **Output generation.** After the model generates a preliminary synthetic output based on its trained parameters, the output will go through several renderings for quality enhancement (such as smoothing transitions between frames).
5. **Quality control.** After quality enhancement, the output goes through final testing and must meet certain criteria depending on the application in question. If the output does not meet the requirements—which are usually objective measurements—it will enter a feedback loop, which is a process to improve the model's performance based on the final product (it learns from its mistakes and tries again). If it meets the criteria, the model considers the output a sufficient deepfake and delivers it to the user.

Deepfakes can be detected due to the imperfections of the process described above. Here is what to look for (or what your expert will be looking for):

- **Flaws.** There are common patterns and flaws associated with deepfake videos that differ from genuine video content, such as:
 - Inconsistent facial features (mismatched expressions with the underlying video or awkward emotional transitions)
 - Lighting and shadow inconsistencies (e.g., the deepfake may not accurately show lighting on the face)
 - Unusual eye movement or inconsistent blinking
 - Failure of lip-syncing
 - Overlap or blending with background artifacts (e.g., a lamp suddenly appears to take over a portion of a person's face)
 - Unnatural speech patterns

- **Frame consistency.** A video is a series of images (frames), and the rate at which the frame changes may be inconsistent or otherwise disturbed in a deepfake video.

Related Content

For a full listing of current practical guidance materials on generative artificial intelligence (AI), ChatGPT, and similar tools that is organized by practice area and updated with new developments, see

 **GENERATIVE ARTIFICIAL INTELLIGENCE (AI) RESOURCE KIT**

For key resources that provide step-by-step guidance on fundamental civil litigation tasks that an attorney will typically work on when litigating a case in federal court, see

 **CIVIL LITIGATION FUNDAMENTALS RESOURCE KIT (FEDERAL)**

For a discussion on how to make pitches for new litigation business, including preparing the presentation, effective communication techniques, and following up after the pitch, see

 **LITIGATION BUSINESS PITCHES: FIVE TIPS**

For an examination of the ethical issues litigators must be aware of when considering using generative AI technology in their practices, including the many ways litigators may use AI and the specific professional ethics rules that apply, see

 **AI AND LEGAL ETHICS: WHAT LAWYERS NEED TO KNOW**

For an analysis of the primary issues relating to the use of ChatGPT or other chatbot AI programs in the practice of law, see

 **LAWYERS AND ChatGPT: BEST PRACTICES**

For a review of the expectations and opportunities for a senior litigation associate, such as leading case teams, interacting with clients, developing a niche, and strategies for success, see

 **PROFESSIONAL DEVELOPMENT: LIFE AS A SENIOR LITIGATION ASSOCIATE**

For guidance on the utilization of AI to measure an outside litigation counsel's performance and using new tools to expedite and enhance the delivery of legal services, see

 **AI AND THE EVALUATION OF OUTSIDE COUNSEL**



Note that metadata comes in all forms and provides all sorts of information about electronic files. In this context, there are several types of metadata that can be helpful in spotting a deepfake, such as the following:

- Creation metadata such as a timestamp will tell you when the video was created. You can then crosscheck the timestamp date with the date your proponent contends the video was taken. Similarly, if the metadata shows the device information, that will help you verify the source.
- File type, size, and other details found in the file metadata can provide additional context. Deepfake files tend to be bigger due to their complexity.
- Modification history is sometimes maintained in the metadata, and it may suggest tampering and even reveal what software was used for editing.
- Geolocation can tell you if the content matches the location where the event allegedly occurred.
- Original source information, if available, might show who created the original or whether there is a watermark (sometimes there are invisible data stamps that may reveal ownership rights or the software it was made with). If the author is shown as unknown or anonymous then, at the very least, you may want to inquire further.

Detection Technologies

Several deepfake detection technologies are currently available, and they can be divided based on their underlying methodology and technology as such:

- **Deep learning approaches such as convolutional neural networks or recurrent neural networks.** These are types of machine learning programs that use large datasets to learn

Some websites, forums, and social media communities are dedicated to identifying common scams, including deepfakes.

patterns characteristic of genuine media. These models then analyze new media to identify similar patterns or detect anomalies that may indicate manipulation. In other words, the type of technology making the deepfakes is also being used to detect them. These programs include:

- Sensity AI¹² is a popular technology used to scan videos and images for signs of manipulation, such as unnatural movements or inconsistencies in background elements.
- FaceForensics++,¹³ although not a commercial solution for detection like Sensity AI, is a research-based tool to train detection technologies like Sensity AI. FaceForensics++ offers companies and developers a large dataset of manipulated videos to train deep learning networks to detect deepfakes.
- **Biometric and behavioral analysis.** These focus on human traits that are difficult to fake such as voice biometrics. Such programs include:
 - Phoneme-Viseme Mismatch¹⁴ checks if lip movements match the corresponding spoken audio. An analyst can do this manually (with the human eye) or the approach can be supported by machine learning.

- Intel’s FakeCatcher¹⁵ works by analyzing blood flow in video pixels to determine if the person is real (because when a heart pumps blood, veins change in color).¹⁶
- **Digital forensic techniques.** These refer to tools that focus their analysis on signs of media alteration or tampering—usually by examining the metadata or visual inconsistencies. Programs include:
 - Amped Authenticate¹⁷ is self-described as a photo and video analysis and tampering detection tool. The software is designed to unveil the processing history of a digital image or video to determine whether a medium is an unaltered original, an original generated by a specific device, or the result of manipulation using editing software. Amped Authenticate¹⁸ generates a detailed scientific report that it claims is admissible in court.
 - Pindrop¹⁹ analyzes audio to provide a “liveness” score. Pindrop also offers a tool called Phoneprinting™, which detects subtle anomalies with acoustic features. Similarly, the company offers Toneprinting™, which allows for the authentication of customers by pinpointing their devices and matching phone numbers.

- **User feedback and internal authentication analysis.** Some websites, forums, and social media communities are dedicated to identifying common scams, including deepfakes. Such media may contain its own digital marks (such as a watermark) for the very purpose of authentication. Examples include:
 - Blockchain technology, such as Bitcoin, uses cryptographic keys to ensure that no one can access or alter the data contained on the ledger (i.e., the blockchain) and it also requires any changes to be verified by multiple nodes through algorithms (i.e., it is self-authenticating). One blockchain technology in the media context is OriginTrail,²⁰ which leverages blockchain technology to manage and verify digital assets, such as a video or image.
 - Content authenticity initiative is a collaborative effort aimed at ensuring authenticity of media in today’s deepfake world. Adobe has taken the lead and has developed a feature known as Content Credentials,²¹ found in Adobe’s creative software, which embeds metadata into digital content, documenting its origins and any modifications.

12. Sensity AI: Best All-In-One Deepfake Detection. 13. GitHub - ondyari/FaceForensics: Github of the FaceForensics dataset. 14. Shruti Agarwal, Hany Farid, Ohad Fried Maneesh Agrawala, Detecting Deep-Fake Videos From Phoneme-Viseme Mismatches, CVPR Workshop Paper (2020).

15. Intel Introduces Real-Time Deepfake Detector (Nov. 14, 2022). 16. David Salazar, How Intel Putting its, AI-optimized Processors to Work Detecting Deepfakes. Fast Company (Oct. 3, 2023). 17. Amped Authenticate - Photo and Video Analysis and Tampering Detection. 18. Setting the Standard for Image and Video Forensics, Amped Software. 19. Privacy - Pindrop. 20. OriginTrail. 21. Discover how creators can use Content Credentials to obtain proper recognition and promote transparency in the content creation process

Best Practices for Evidence Collection and Discovery

At the outset of a case, you should have discussions with your staff about potential fabricated evidence and how other evidence can be obtained to prove it. You should collect and preserve corroborating evidence, such as geolocation data and phone records. For example, you may need your client’s telephone records to help authenticate a recording with the defendant if it is called into question.

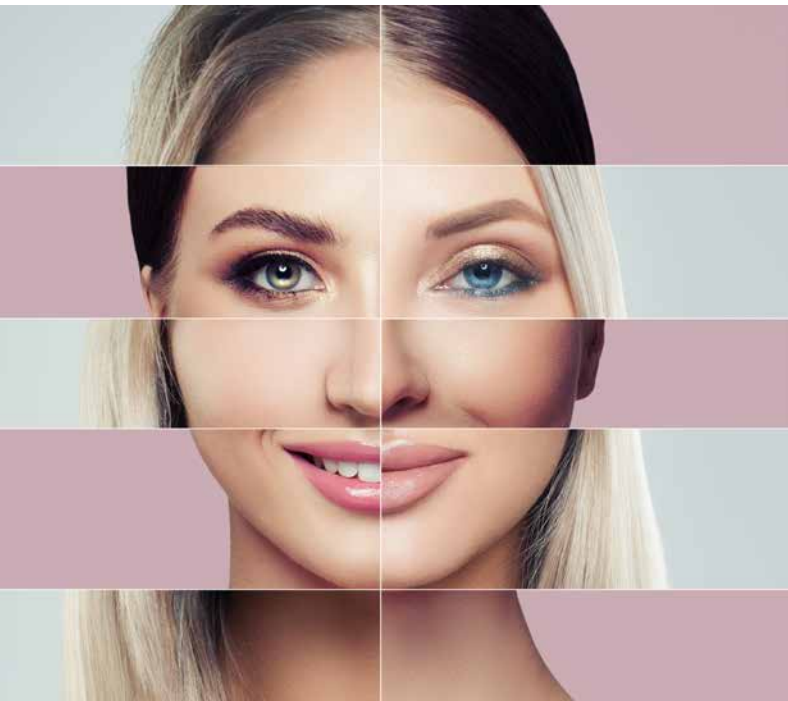
You should also seek out contrasting evidence, such as photos of an alleged video participant. This can be used to impeach authenticity. In addition, secure the location of evidence, such as the location of where digital records are stored, including the names and locations of custodians of the records.

Chain of custody information is crucial for supporting or challenging digital evidence as fake. How the witness obtained and maintained the evidence can be best shown through metadata. To obtain metadata, you must obtain the files in native form.

Your staff should be monitoring the following as a first line of defense to deepfake evidence:

- Metadata, such as storage history, transfer history, edits, watermarks, file size, and other corroborating evidence
- Visual inconsistencies, such as unnatural lighting or shadows, blurry areas, inconsistent skin tone or texture, background anomalies, and neck and lip movement that is not aligned with audio
- Lack of corroborating evidence

Talk to your client about the potential evidence in the case to help you identify any specific evidence to look out for. If there is any anticipation of a deepfake, do not delay—have a list of forensic experts ready and work with one as soon as the need arises. Make sure your client understands that an allegation of deepfake



Related Content

For an overview of the integration of AI into law firm management and performance, see

 [HOW TO USE AI TO MANAGE THE ATTORNEY-CLIENT RELATIONSHIP](#)

For practical tips for an attorney relocating to another firm, including what to consider when considering a lateral move and how to navigate your ethical responsibilities, see

 [LATERAL MOVES FOR ATTORNEYS: WHAT YOU NEED TO KNOW](#)

For information on managing a litigation client's expectations, including the initial client meeting, early case assessment, engagement agreements, budget and billing, communicating with the client during the litigation, and post-litigation reviews, see


 [MANAGING CLIENT EXPECTATIONS IN LITIGATION](#)

For assistance in drafting client memos and emails, covering such topics as effective drafting techniques, preserving privileges, and maintaining the security of your client communications, see

 [DRAFTING CLIENT MEMOS AND EMAILS](#)

For a look at the primary and emerging legal issues related to AI, see

 [ARTIFICIAL INTELLIGENCE KEY LEGAL ISSUES](#)

evidence can increase costs. In addition, you should pursue deepfake detection tools, such as the examples above, for an initial assessment of the questionable evidence. 

Bijan Ghom is senior counsel at Saxton & Stump. He handles commercial litigation, business and corporate law, intellectual property, and trusts and estates litigation. A former business owner with a master’s degree in business administration, he continually works with business clients to assist with litigation and intellectual property. He brings his experience founding and selling a number of businesses to advising his clients on protecting and monetizing intellectual property assets. He is also a strategist with Palq IP, an IP strategy firm and strategic partner of Saxton & Stump.

 [RESEARCH PATH: Civil Litigation > General Litigation > Practice Notes](#)



BROADEN
YOUR
HORIZON
SCANNING

See further with Law360[®] and Lexis+[®]
Anticipate change and act with confidence using breaking business and legal news, trusted Practical Guidance content and AI-powered resources.

Visit [lexisnexis.com/cl-horizon-law360](https://www.lexisnexis.com/cl-horizon-law360) or call 800-628-3612.





Romaine Marshall and Jennifer Bauer POLSINELLI PC

AI Risk Management in the United States: Looking Ahead

This article addresses the broad scope of artificial intelligence (AI) laws in the United States that focus on mitigating risk.

ALREADY, AI GOVERNANCE CONSISTS OF A GROWING patchwork of laws, regulations, and industry standards that are beginning to form duties of care and other legal obligations. Many of these are narrowly tailored to address specific AI risks or pre-existing laws that are being applied in a new context, even if they are not AI-specific.

In lieu of a well-regulated industry with established legal frameworks around AI, professionals interested in mitigating AI risks within their businesses will need to consider other signals to identify, evaluate, and mitigate AI risk. In addition to evolving state laws, authoritative sources/signals include Federal Trade Commission (FTC) enforcement trends/cases and the National Institute of Standards and Technology's AI Risk Management and Cybersecurity Frameworks (NIST AI RMF and NIST CSF).

When combined and viewed holistically, this patchwork of AI laws, enforcement trends, and industry guidance result in some clear AI risk management techniques for business professionals to consider.

NIST AI Risk Management Framework

The NIST AI RMF¹ defines an AI system as a system that generates outputs influencing environments.

The NIST AI RMF offers voluntary guidance to individuals and companies on managing risks that AI poses in various contexts throughout its life cycle in order to deploy and use trustworthy AI models. Trustworthy AI characteristics, as defined by NIST, include:

- Validity
- Reliability
- Safety
- Security
- Resilience
- Accountability
- Transparency
- Explainability
- Interpretability
- Privacy enhancement
- Fairness

While balancing the above characteristics depends on the AI's use case, neglecting these characteristics can increase the probability



and magnitude of negative consequences. NIST recognizes that the AI RMF is meant to operate as a flexible guide to approaching risk, and approaches may change as more research is completed and companies provide feedback.

The AI RMF defines risk as a composite measure of an event's probability of occurring and the magnitude of the consequences of the corresponding event regardless of whether they are negative or positive. Unlike past frameworks, the AI RMF focuses on minimizing anticipated threats and opportunities to maximize positive impacts.

The AI RMF covers how companies can govern, map, measure, and manage their enterprise, consistent with previous frameworks like the NIST CSF and its newer version (2.0)² released in early 2024. A company's capacity for risk tolerance is unique, but the AI RMF suggests several risk-management techniques companies can employ to start their risk management program:

- AI risk management policy
- Inventory of AI systems
- AI impact assessment template
- AI system performance and monitoring template
- AI system risk register
- AI incident response plan
- Third-party risk management
- AI risk management training
- Channels to receive AI updates

1. National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile* (July 2024). 2. National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0* (Feb. 26, 2024).

While the AI RMF acknowledges that there is a spectrum of risk involved in AI systems based on their intended use, and that there are AI systems that can pose unacceptable risks and should not be deployed until those risks are mitigated, it does not specify what those use cases might be or provide corresponding risk thresholds. The Generative AI Profile³ clarified 12 distinct threats unique to or exacerbated by AI across life cycle stage, scope, source, and timescale as verified by existing empirical evidence. The Profile was designed to help organizations identify AI-specific risks and limits its

guidance to industry-agnostic tools through which organizations can make their own risk identification and mitigation determinations. The applicable use case requires a practical interpretation of the broad risks proposed. The accompanying NIST CSF 2.0 Implementation Examples⁴ provide greater clarification. A high-level overview of the risk management techniques, risks, and controls we typically recommend including in such a program is enclosed in the below visual.

3. The NIST Cybersecurity Framework (CSF) 2.0. 4. National Institute of Standards and Technology, CSF 2.0-Implementation Examples.

Federal Trade Commission Enforcement Action

The FTC has been actively taking action against the improper use and development of AI. In December 2023, the FTC filed an enforcement action⁵ against Rite Aid Corporation for improper use of an AI system they deployed to catch shoplifters. The FTC found that Rite Aid did not take the proper precautions surrounding customer data and biometric data by failing to:

- Mitigate potential risks
- Measure the accuracy of the system that was deployed
- Prevent low-quality data from being used
- Properly train employees on how to use the system

Rite Aid later agreed, in a stipulated order⁶ with the FTC, to conduct a system assessment every 12 months as part of the surveillance system monitoring program, along with other requirements commonly seen in a written information security program.

In February 2023, the FTC issued a statement, more of a warning, that companies who adopt more permissive data practices without notifying customers, or notifying them retroactively, may be engaging in unfair or deceptive practices. 1Health.io Inc. settled with the FTC in September 2023 after violating the statement above.⁷ 1Health touted sharing customer’s health information and genetic information in limited circumstances, along with deleting the data whenever asked.

The FTC found that 1Health lied by retroactively changing their privacy policy to include third parties without notifying customers of this change as required by law. Despite receiving multiple warnings, 1Health failed to change their practices, leading to the eventual settlement requiring 1Health to implement a robust information security program, prohibiting them from sharing health data with third parties (including information prior to 2020), and requiring them to report all future incidents to the FTC.

State Approach to AI Governance

In the absence of a federal law, states have taken the initiative to add their own laws to the patchwork covering a wide variety of topics. When AI became a hot topic in 2023, many states passed legislation directing task forces to investigate AI risks and usage or assigned an existing office to oversee research on AI use in specific industries. A few states have taken action to mitigate risk in private industry. Utah is the first state to have an active AI bill amending its current consumer protection and data privacy laws to ensure transparency of AI usage.⁸ Essential industries, such as healthcare and finance,

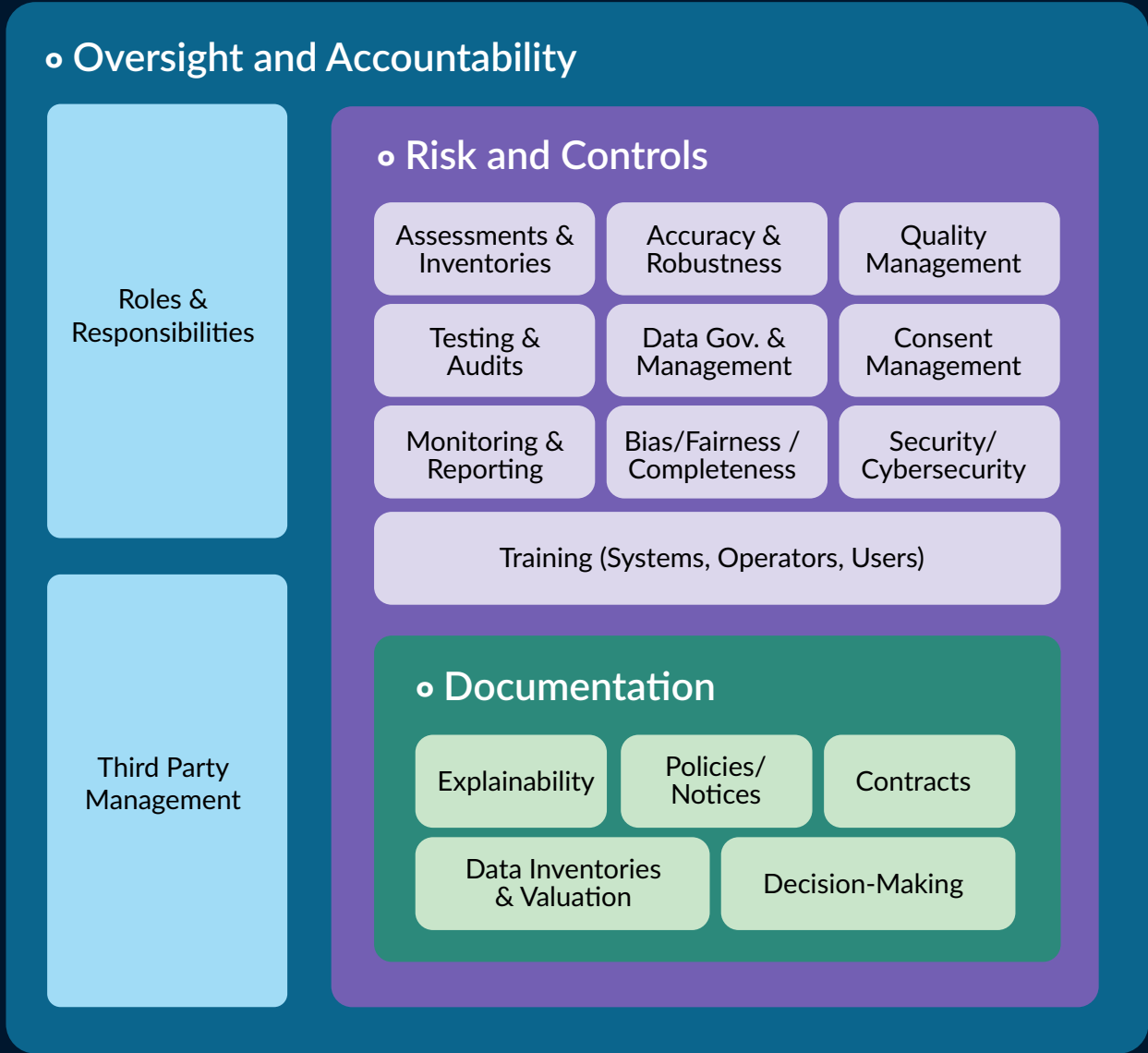


must make available on their website a disclosure notifying consumers of AI usage and before they interact with an AI system. Current data privacy laws have been amended to include the definition of synthetic data, which would include any answers created by AI. Yet, Utah is taking a research then legislate approach by creating the Utah AI Policy Office to guide AI research, development, and future legislation.

This office will also operate as a sandbox for companies who want to develop AI systems in Utah. The AI Policy Office is also required to develop cybersecurity standards and other regulatory requirements for these companies to follow, but much is to be determined on this. Other states, like Colorado, have more robust mitigation techniques in place. Heavily influenced by the NIST AI RMF, the Colorado AI Act⁹ applies to developers and deployers of high-risk AI systems. A developer is an entity or individual that develops or intentionally and substantially modifies a high-risk AI system and a deployer is an individual or entity that deploys a high-risk AI system.¹⁰ The Act requires that deployers and developers meet certain criteria as seen below and have a reasonable duty of care to protect consumers from known or foreseeable risks:

5. FTC v. Rite Aid Corp., No. 23-cv-5023 (E.D. Pa. Dec. 19, 2023). 6. FTC v. Rite Aid Corp., No. 23-cv-5023 (E.D. Pa. Feb. 26, 2024). 7. 1Health.io Inc., 2023 FTC LEXIS 77 (Sept. 6, 2023). 8. See Utah Artificial Intelligence Policy Act, Utah Code Ann. §§ 13-72-101 to -305. 9. Colo. Rev. Stat. §§ 6-1-1701 to -1707. 10. Colo. Rev. Stat. § 6-1-1701(6) and (7).

Risk Management Techniques and Controls





DEVELOPER	DEPLOYER
<ul style="list-style-type: none">■ Must make certain documentation available for deployers as recommended by the NIST AI RMF. Documents must disclose:<ul style="list-style-type: none">• Type of data used to train the system• Known or foreseeable limitations of the system• Purpose and intended benefits of system■ Documents must cover:<ul style="list-style-type: none">• How the system was evaluated for performance• Measures taken to mitigate algorithmic discrimination• How the system should be used, not used, and monitored• Data governance measures used to cover training data• Intended outputs• Any other documentation required to understand the outputs and monitor performance■ Must clearly display on their website or in a public place a summary of how they manage the risks of algorithmic discrimination that may arise from the development, modification, or deployment of their AI system■ Within 90 days of discovering, or learning from a credible source, that their high-risk AI system has caused or is reasonably likely to cause algorithmic discrimination, must inform the CO attorney general and all known deployers of the system¹¹	<ul style="list-style-type: none">■ Must use reasonable care to avoid known or reasonably foreseeable risks of algorithmic discrimination■ Must conduct annual impact assessments, as well as within 90 days of each intentional and substantial modification of the system■ Must notify customers when they have deployed a high-risk AI system to make—or be a substantial factor in making—a consequential decision about the customer before the decision is made■ Must make certain disclosures available on their website

11. See Colo. Rev. Stat. §§ 6-1-1702 to -1704.

When combined and viewed holistically, the patchwork of AI laws, enforcement trends, and industry guidance can be distilled into several key takeaways....

Uniquely, Colorado's Attorney General will have complete enforcement authority.¹² Colorado's law may pertain to all industries; however, education, employment, finance, healthcare, housing, insurance, and legal industries are pointed to as involving consequential decisions.¹³ Colorado's law will not be effective until 2026.

California was the most recent state to pass their own flurry of AI bills ranging from building on existing laws to AI use in specific industries. While not as robust as Colorado, 2024 CA AB 2013 will require companies to disclose information on their models and the data set the model was trained on. 2024 CA SB 942 requires developers of AI systems to allow visitors of their system to mark AI generated content and make available tools to identify AI content produced by their systems.

Along with the above, the Office of Emergency Services will partner with OpenAI and Anthropic to conduct risk assessments on AI effects in critical industries. Both laws are effective January 1, 2026.

Holistic AI Risk Management

When combined and viewed holistically, the patchwork of AI laws, enforcement trends, and industry guidance discussed above can be distilled into several key takeaways professionals should focus on when developing their AI risk management strategy.

1. Think about AI risks and laws expansively.

In a legal and regulatory environment that is still evolving, professionals cannot rely on a formal framework or comprehensive AI-specific law, or even a set of AI-specific laws, to define the risks and corresponding mitigation techniques required. Nor can they rely on the term AI being used in the bill or law to indicate its applicability.

Indeed, the risk surface professionals need to manage within the AI context is as expansive as AI is multi-dimensional and cross-functional, and often depends on the specific context and use case in which AI is being deployed. For example, does the use case

12. Colo. Rev. Stat. § 6-1-1706. 13. See Colo. Rev. Stat. § 6-1-1701(3).

involve AI to replicate an actor or musical performer's likeness, voice, and/or behavior?

If so, it likely implicates state laws around the right to publicity (including, e.g., recent laws in California and New York). There are a variety of state laws (discussed above) that are narrowly tailored to address AI-specific risks that have risen to the forefront of public discourse.

Related Content

For more practical guidance on artificial intelligence (AI), see

 [GENERATIVE ARTIFICIAL INTELLIGENCE \(AI\) RESOURCE KIT](#)

For an overview of proposed or pending AI-related federal, state, and major local legislation across several practice areas, see

 [ARTIFICIAL INTELLIGENCE LEGISLATION TRACKER \(2024\)](#)

For a survey of state and local AI legislation across several practice areas, see

 [ARTIFICIAL INTELLIGENCE STATE LAW SURVEY](#)

For a discussion of legal issues related to the acquisition, development, and exploitation of AI, see

 [ARTIFICIAL INTELLIGENCE KEY LEGAL ISSUES](#)

For an analysis of the key considerations in mergers and acquisitions due diligence in the context of AI technologies, see

 [ARTIFICIAL INTELLIGENCE \(AI\) INVESTMENT: RISKS, DUE DILIGENCE, AND MITIGATION STRATEGIES](#)

For a look at legal issues arising from the increased use of AI and automation in e-commerce, see

 [ARTIFICIAL INTELLIGENCE AND AUTOMATION IN E-COMMERCE](#)

For a checklist of key legal considerations for attorneys when advising clients on negotiating contracts involving AI, see

 [ARTIFICIAL INTELLIGENCE \(AI\) AGREEMENTS CHECKLIST](#)

However, focusing on AI-specific laws artificially limits the legal risks to AI-related practices since regulators like the FTC are broadly interpreting existing laws and mandates to encompass the technology. Indeed, many of our federal and state laws focus on industry rather than technology scope and can therefore be applied to AI-related practices.

As evidenced by the FTC enforcement actions and trends discussed above, businesses must therefore think expansively about AI risks and laws that might apply to their AI-related practices before implementing them.

2. Use holistic solutions like those outlined in the NIST AI Risk Management Framework.

Businesses need practical guidance around AI risk management. In lieu of a comprehensive legal or regulatory framework, the NIST AI

RMF can offer businesses a systematic vehicle through which to identify, evaluate, and mitigate AI risks within their organization. It also demonstrates how businesses can use well-established risk management techniques like risk assessments, testing, and documentation to manage AI risks.

The sheer volume and variety of risks involved in AI will require businesses to incorporate AI within their broader enterprise-wide risk management programs.

While voluntary, the FTC’s frequent reliance on NIST as a barometer of industry standards increases the likelihood that the NIST AI RMF will become a comparative benchmark over time. And it does an admirable job of summarizing the variety and volume of risks and controls businesses should consider when building their AI risk management programs.

Doing so will help reduce business risk even as the United States continues to build and refine its AI laws and regulations in today’s patchwork environment/landscape.

3. Always involve humans in any AI-enabled processes and decision-making.

Most risks associated with AI can be mitigated via human intervention, including:

- Verifying the completeness and accuracy of its data inputs
- Testing and validating its results
- Limiting use cases to appropriate parameters
- Interpreting results in context to mitigate bias -and-
- Preventing harmful effects like obscene, degrading, and/or abusive content (like non-consensual intimate images)

If a business were to consider implementing only one technique for mitigating AI risk, embedding human intervention throughout the AI lifecycle would offer the highest value for concentrated effort.

If nothing else, embedding humans in any AI-enabled processes and decision-making will ensure line-of-sight into the resulting operations and limit the business’s reliance on an AI system or algorithm as part of any contested decision (see, e.g., the many state laws focused on automated decision-making discussed above and the corresponding right of individuals to request explanations of the factors and accuracy of the algorithm involved).

4. The best solution is often the simplest: Be proactive and transparent in soliciting informed consent.

When all else fails, informed consent is one of the best forms of authorization available to businesses, especially when the corresponding legal and regulatory frameworks are evolving. But the key to success is ensuring the consent is accompanied by the requisite notice and disclosures to support it, which can often turn on the transparency and timing of that notice and consent.

Consider iHealth’s settlement with the FTC (discussed above) a cautionary tale of the dangers of retroactive privacy notice changes and historical data usage. While it may sound basic, businesses should never retroactively post changes to their privacy notice or website terms and conditions or use historical data based on those updates without clear, informed consent from the individual involved!

It is a recipe for FTC enforcement in this environment, especially given the agency’s public statements. When executed well, however, proactive and transparent notice and consents can offer the best foundation for businesses operating in evolving legal and regulatory frameworks. **L**



Romaine Marshall is a shareholder at Polsinelli PC. He helps organizations navigate legal obligations relating to data innovation, privacy, and security. He has extensive experience as a business litigation and trial lawyer, and as legal counsel in response to hundreds of cybersecurity and data privacy incidents that, in some cases, involved litigation and regulatory investigations. He has been lead counsel in multiple jury and bench trials in Utah state and federal courts, before administrative boards and government agencies nationwide, and has routinely worked alongside law enforcement.

Jennifer Bauer is counsel at Polsinelli PC. She has extensive experience in global privacy program design, evaluation and audit, regulatory compliance and risk reporting, remediation, and data privacy and cybersecurity law. She is a trusted and experienced leader certified by the International Association of Privacy Professionals. Jenn has transformed the privacy programs of five Fortune 300 companies and advised blue-chip companies and large government entities on data privacy and security requirements, regulatory compliance (particularly GDPR / CCPA), and operational improvement opportunities.



Emily Schifter TROUTMAN PEPPER LOCKE

Key AI Legal Issues in DEI & Employment Discrimination

This article provides guidance and best practices for counseling employers on key employment discrimination and diversity, equity, and inclusion (DEI)-related legal issues associated with using artificial intelligence (AI) tools.

AI and Generative AI

This section briefly explains a few basics about AI and generative AI technology as potentially relevant to employers.

While there is no standard definition of AI, the term AI can be generally used to describe any technology that allows a machine to perform tasks in a manner that simulates human intelligence. For instance, the National Artificial Intelligence Initiative Act of 2020 defines AI to mean a “machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environment.”¹

Generally, AI-powered tools are designed to execute algorithms (a set of instructions or code that a computer follows to accomplish a given task) over a data set. Some AI programs (known as machine learning) even can learn, or improve their ability to perform certain tasks better or faster over time based on their experience.

AI-powered technology may have the ability to:

- Identify patterns
- Make conclusions
- Predict future occurrences or behavior
- Make informed judgments
- Automate certain functions



Generative AI takes this all one step further—as its name suggests, this type of AI can generate novel content on its own, including text, images, and even video or audio. Perhaps the most well-known example of a generative AI tool is a large language model (LLM) (e.g., ChatGPT). These tools are trained on large amounts of text. The LLM will read and incorporate everything on which it is trained, then use the information to predict the most statistically likely next word, sentence, or paragraph in a given context. This allows an LLM to generate human-like narrative responses to questions, based on the information they have been trained on.

How Employers Are Using AI

Employers are likely already using many AI-powered tools, perhaps without realizing it. For instance, employers commonly use programs that screen resumes or job applications for key words or phrases. Or they may use scheduling software that has the ability to analyze patterns to optimize staffing. Still others are beginning to incorporate AI tools in their day-to-day substantive work. While this is a fast-developing area with new tools (and potential risks with existing tools) being identified frequently, this section addresses some of the common ways that employers may use AI for recruiting and hiring, employee evaluation, employee engagement, and their substantive work.

Recruiting and Hiring

One of the most common ways employers have historically used AI tools is in the recruiting and hiring space. Traditionally, for example, employers have used resume screeners to identify key words corresponding with the skills and experience desired for a given job opening from the many resumes or applications they may receive. But this is also an area where many new tools are being released that go beyond a simple screening tool, such as video-interviewing software and programs that trawl career websites to proactively identify prospective candidates for a given job opening and encourage them to apply.

The hiring and recruiting space is also one of the first areas where legislatures have been moving to create laws and

guidance to limit the use of AI tools in ways that may create the risk of discrimination, and where litigation over purported discrimination resulting from the use of such tools has already begun to pop up, as discussed below.

Specific examples of AI tools that employers may use for recruiting and hiring efforts include:

- Screeners that scan applications or resumes for certain key words
- Tools that help draft or optimize job postings
- Tools that search career websites or social media for candidates and engage in job advertisements or candidate targeting
- Chatbots that perform some of the initial information-gathering about potential job applicants by asking those applicants about their qualifications
- Tools that help schedule interviews with candidates who have passed an initial screening
- Video-interviewing software that evaluates candidates based on facial expressions and speech patterns
- Testing software that is used to assess potential job applicants’ skills, aptitude, or ability

¹ Pub. L. No. 116-283, § 5002, 134 Stat. 3388 (Jan. 1, 2021).

AI tools can help employers accomplish rote tasks faster and more accurately. Because more data can be reviewed in a shorter period, employers are freed up to spend more time on higher-level work.

Employee Evaluation

As more and more AI tools continue to be developed, employers have also begun to incorporate AI tools into the processes they use to evaluate their employees. Specific examples of some of these tools include the following:

- **Performance evaluation.** Performance evaluation tools that assist in monitoring employee performance and even provide a first draft of a performance evaluation.
- **Keystroke monitors.** Keystroke monitors, cameras, or other tools that monitor employees' work, especially remote employees.
- **Market data.** Tools that help analyze market data or data within a given employee population to identify market or pay equity trends or issues, recommend pay changes, or inform salary offers to new hires.

Employee Engagement

Some employers are also using AI tools to help them retain and support their existing employee populations. Specific examples of some of these tools include the following:

- **Workforce optimization tools.** Workforce optimization tools that assist in scheduling employees based on customer, staffing, or other data trends.
- **Worker management software.** Worker management software, including tools that help review time off and leave requests, assist with open enrollment, or make simple updates to employee information.
- **HR chatbots.** Chatbots that answer simple human resources questions from employees about policies and procedures.
- **Drafting tools.** Drafting tools that help prepare form or other basic documents, such as offer letters.

Substantive Work

Of course, employers might also be employing various AI tools in their day-to-day work itself, and employees, both with and without employer knowledge or permission, might be doing the same.



Potential Anti-discrimination and DEI-Related Benefits to AI

Many employers have increasingly turned their focus to enhancing their DEI and anti-discrimination efforts, striving to improve their ability to attract, retain, support, and promote diverse individuals. This section addresses potential ways that employers might benefit from using AI to achieve their DEI-related and anti-discrimination objectives.

Here is a brief overview of DEI:

- **Diversity** refers to the types of people who make up a workforce and can include a variety of types of diversity—gender, race, age, sexual orientation, physical ability and neurodiversity, or other characteristics, as well as, sometimes, even characteristics not traditionally protected by employment discrimination laws, such as diversity of viewpoint, experience, or opinion.
- **Equity** refers to the aim of treating all people fairly, rather than differentially, based on identity, with the goal that all people are ultimately treated equally.
- **Inclusion** refers to ensuring all individuals in a workplace feel included and supported. Note that DEI is also often rephrased as DEIB, to incorporate the related concept of belonging.

AI tools can help employers achieve their DEI-related and anti-discrimination goals in several ways.

Lack of Bias

One potential benefit of AI tools as opposed to traditional human review is that at least in theory, they should be without

bias. After all, algorithms do not have the same experiences that humans do that may cause them, explicitly or implicitly, to value candidates or employees of certain identities over others, such as the unconscious bias toward individuals that employees sometimes feel in favor of those individuals who they feel are similar to themselves.

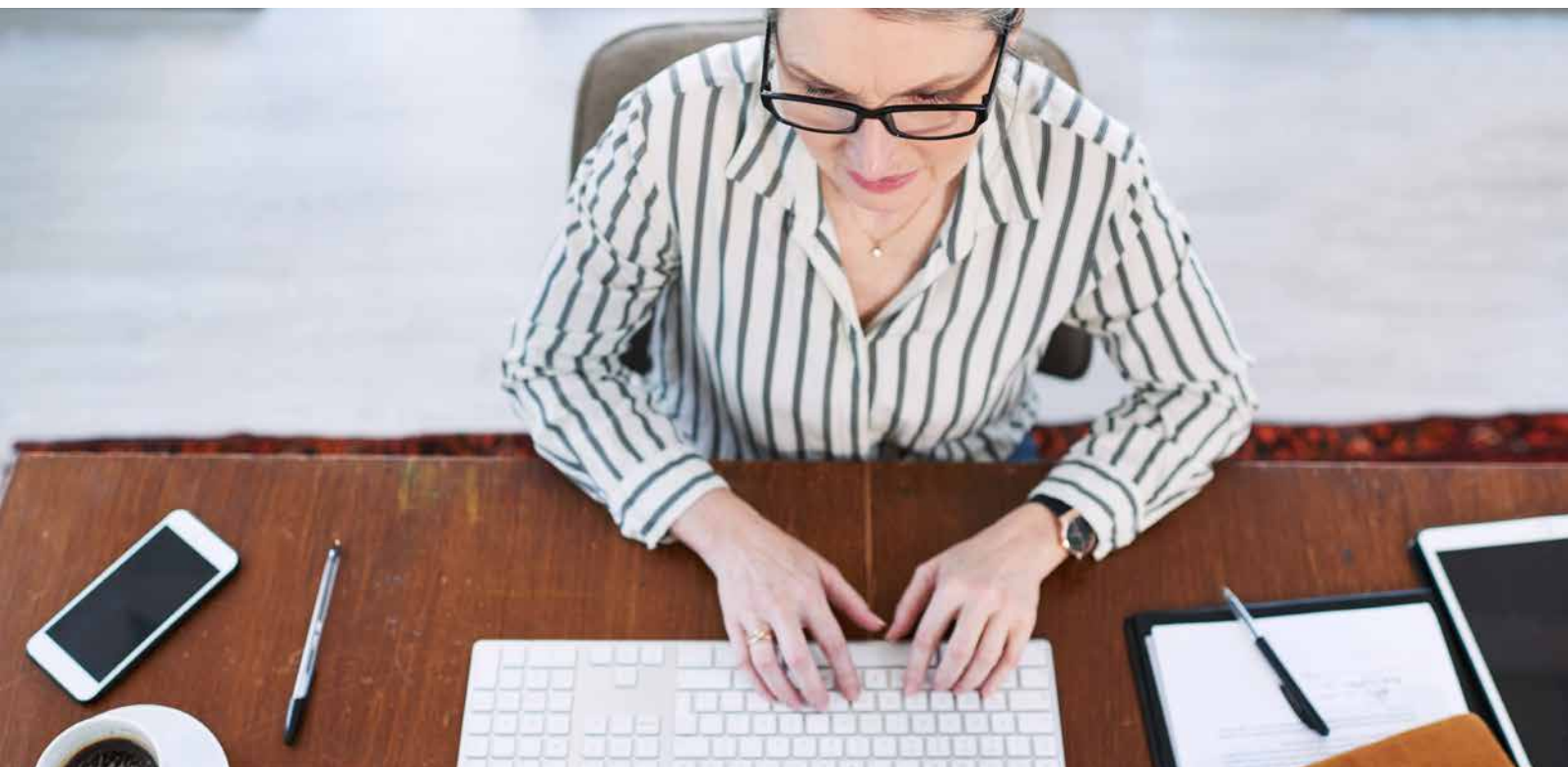
Efficiency and Reach

AI tools can help employers accomplish rote tasks faster and more accurately. Because more data can be reviewed in a shorter period, employees are freed up to spend more time on higher-level work. Further, AI can unlock insights and trends in data that a human might miss.

Practically, for example, this might mean that while a traditional recruiter may cease to review resumes after reaching a certain number, a scanner program can review the full slate. That might both free up a recruiter's time to consider diverse candidates more thoughtfully, or even unearth candidates that the recruiter might not have otherwise considered. By way of further example, an AI-powered tool might help identify retention problems among individuals of a particular background or roles over time or unearth inequities in salary levels that were not immediately apparent to a management team.

Support

Employers can use AI tools to offer training, career path guides, or other employee-specific tools to help employees of all identities advance their careers, improve skills, or be matched with appropriate job opportunities.





Potential Discrimination and DEI-Related Risks to AI

Though when used thoughtfully, AI can help employers improve their anti-discrimination and DEI efforts for all the reasons noted above, there are also certainly many potential risks. This section details some of those risks and outlines considerations for counsel advising employers on their use of these tools.

Discrimination

Perhaps the biggest DEI-related risk associated with the use of AI tools is potential employment discrimination. This section addresses the types of discrimination claims most potentially relevant to employers’ use of AI tools, the ways that AI-powered tools might increase the risks of or contribute to such claims, and some practical considerations regarding the risks of such claims in this context.

Types of Discrimination

Federal and state laws governing discrimination apply regardless of whether an employer’s employment decisions are performed solely by humans or performed entirely or with assistance of an AI technology. Thus, it is critical that you advise employers using AI tools that they must always have and maintain a solid understanding of their obligations with respect to applicable discrimination laws, and that these obligations do not disappear when deploying an AI tool.

Although a full overview of applicable employment discrimination laws is beyond the scope of this article, there are a variety of federal and state laws that govern employers in this space.

For example, under federal law:

- Title VII of the Civil Rights Act of 1964 (Title VII)² prohibits employment discrimination based on race, color, religion, sex (including pregnancy, sexual orientation, and gender identity), or national origin.
- The Age Discrimination in Employment Act (ADEA)³ prohibits discrimination based on age (40 or over).
- The Americans with Disabilities Act (ADA)⁴ prohibits discrimination based on mental or physical disability.
- The Genetic Information Nondiscrimination Act⁵ prohibits discrimination based on genetic information.

These and other discrimination laws may prohibit two types of discrimination:

- **Disparate treatment.** Intentional discrimination against one individual because of their membership in a class protected by law.
- **Disparate impact.** When a facially neutral policy or practice (including a selection procedure or test) unduly disadvantages individuals based on their membership in a protected class.

Though the use of AI could, in theory, implicate either type of discrimination, it is this second category that creates the biggest trap for the unwary employer. Because it is often difficult to understand why or how an algorithm made a particular decision, it may be more difficult for employees or candidates to show that an employer intentionally discriminated via the algorithm. But that same point may likewise make it harder for an employer to offer a solid nondiscriminatory reason for the decision.

How AI Tools Might Increase the Risk of Discrimination

Thus, an employer acting without discriminatory intent using an AI tool—even an employer using such a tool with the hope of increasing diversity—can still put themselves at risk of discrimination claims due to the nature of the technology itself and the contexts in which it may be used. This section discusses those risks in more detail.

Bias in Data

AI systems are only as good as their inputs. If an AI system is trained on biased or unrepresentative data, it runs the risk of replicating that bias. Existing data sources may reflect prior or existing bias or even just historical underrepresentation of diverse groups. If an AI-powered tool ingests that data as its training source, it may inadvertently amplify, rather than mitigate, such bias. As an AI tool’s algorithm learns, in other words, there is a risk that the model will continue to reflect a lack of representation of underrepresented groups or favor historically represented groups.

For instance, consider an AI tool that is designed to compare job candidates to employees currently successful in those roles. If the current employee population does not contain many diverse individuals, the tool may inadvertently filter out candidates who are diverse or different from the primary group represented. Or consider a facial recognition or speech analysis algorithm trained on data that overrepresents white people, or men, or people without disabilities, which may result in racial bias against people of color, or women, or those with disabilities in the form of less accurate facial recognition or speech pattern recognition results. It is easy to see how this could become problematic in the use of video-interviewing screening software that filters out hundreds of applicants before they ever reach a human recruiter for review.

Bias in Programming

AI systems are also only as good as the humans who create them. Thus, AI bias may also arise from programming errors, wherein a developer may mistakenly place emphasis on certain factors or due to their own biases.

Related Content

For a presentation on environmental, social, and corporate governance employment law issues, see

 [ENVIRONMENTAL, SOCIAL, AND GOVERNANCE \(ESG\) FOR EMPLOYERS AND HR: TRAINING PRESENTATION](#)

For more resources on artificial intelligence (AI), see

 [GENERATIVE ARTIFICIAL INTELLIGENCE \(AI\) RESOURCE KIT](#)

For a general primer on legal issues related to AI, see

 [ARTIFICIAL INTELLIGENCE KEY LEGAL ISSUES](#)

For guidance and best practices for counseling employers on legal implications of AI in the workplace, see

 [ARTIFICIAL INTELLIGENCE IN THE WORKPLACE: BEST PRACTICES](#)

For an analysis of the potential legal and business risks stemming from the use of AI tools to manage employee performance and make employment decisions, see

 [AI IN EMPLOYMENT DECISIONS AND PERFORMANCE MANAGEMENT: KEY LEGAL ISSUES AND POTENTIAL RISKS AND BENEFITS](#)

For a workplace policy regarding AI use by employees and other workers, see

 [ARTIFICIAL INTELLIGENCE \(AI\) DRIVEN TOOLS IN THE WORKPLACE POLICY \(WITH ACKNOWLEDGMENT\)](#)

For a video examining key considerations regarding AI in the workplace, see

 [ARTIFICIAL INTELLIGENCE \(AI\) IN THE WORKPLACE VIDEO](#)

For example, a resume-screening tool might be programmed to automatically reject candidates with gaps of a certain amount of time reflected in their employment history. While a good-natured programmer might believe this would result in filtering out unreliable candidates, it could also easily result in inadvertently filtering out individuals who had to take time out of the workforce due to medical conditions, disabilities, or childbirth. Or consider an algorithm that recruits for new candidates based on location—if the algorithm is

2. 42 U.S.C. § 2000e et seq. 3. 29 U.S.C. § 621 et seq. 4. 42 U.S.C. § 12101 et seq. 5. 42 U.S.C. § 2000ff et seq.

programmed to favor certain zip codes over others, prioritizing historically nondiverse neighborhoods may lead to inadvertent discrimination.

Reliance on Unlawful Information

As noted, AI tools, especially generative AI tools, are trained on large volumes of text. This may include a variety of publicly available text from sources (such as social media or government websites) that may contain information about employees or candidates that employers traditionally should not consider or cannot legally ask about, such as age, sexual orientation, medical conditions, or genetic information.

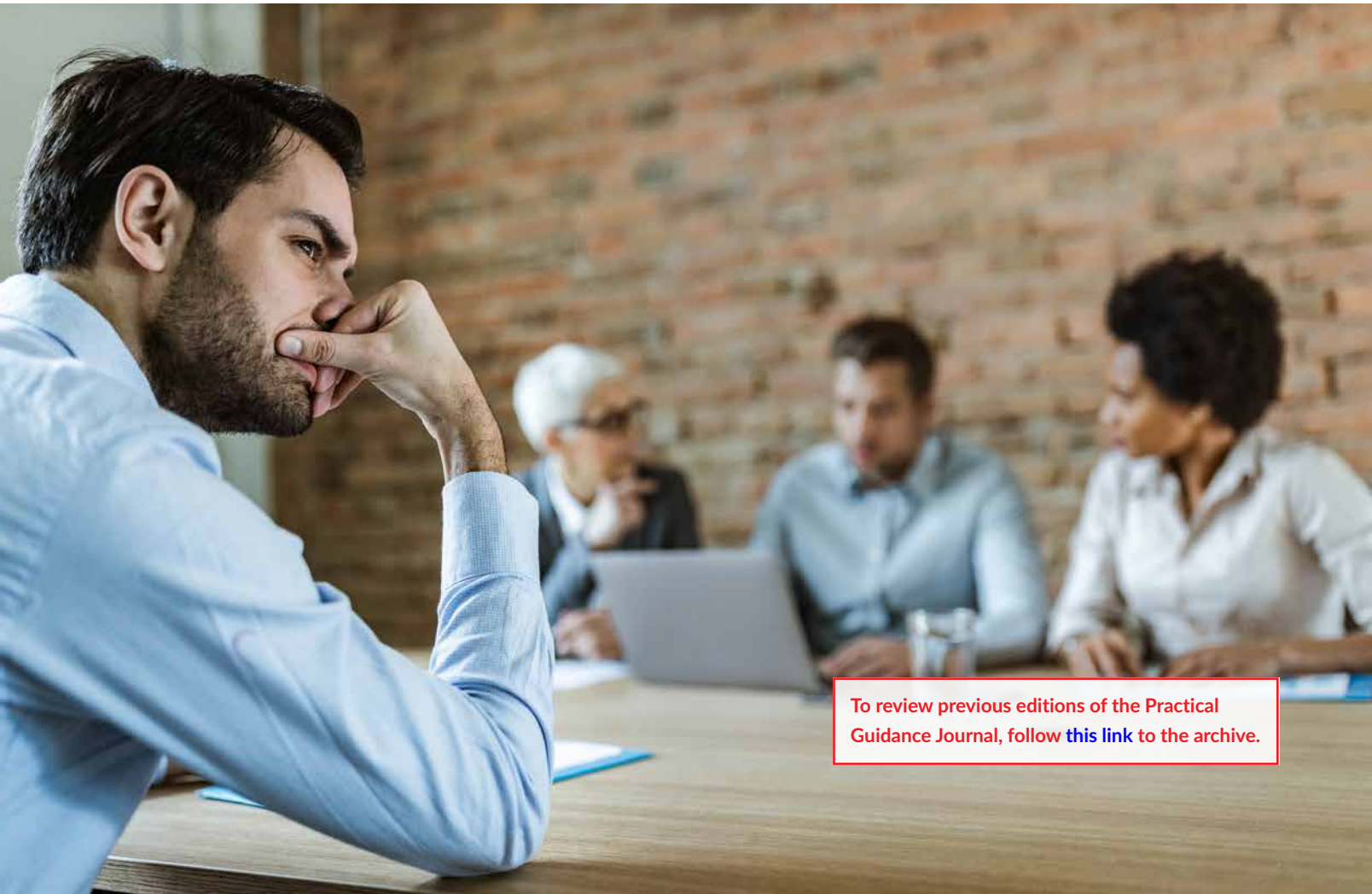
Revealing Potentially Harmful Trends in Existing Data

If an employer uses an AI-powered tool to analyze or assess its existing employee population or data, it’s vital that you counsel them to think critically about what might be learned when the analysis is complete. For instance, a pay analysis tool might reveal that an employer’s pay for a given role is consistently below market. This may be helpful information ultimately, but it can also create employee dissatisfaction. Or such a tool might reveal inadvertent differential treatment among protected classes.

While again, such an insight may be useful to an employer who wishes to move forward with changes to resolve such differential treatment, the existence of such a report could create risk should a current or former employee seek to bring a discrimination claim. Thus, just as with any audit or workforce analysis, you should counsel employers to be prepared that it is possible that data revealed by an AI-powered analysis or audit may reveal more than what they bargained for.

Perception of Bias

Note, too, that even if AI tools used by a given employer have been vetted and tested to ensure they do not contain inadvertent bias, headlines about programs that do contain such bias, and laws and guidance designed to mitigate it, may lend credence to the perception of bias. This may make employees or candidates, particularly those in historically underrepresented groups, wary. Many new tools are coming out quickly, which may further lead to the perception that they are unvetted or may be unfairly or discriminatorily used. To the extent that this makes historically underrepresented groups feel further isolated or marginalized, employers looking to increase their DEI efforts should tread cautiously.



To review previous editions of the Practical Guidance Journal, follow [this link](#) to the archive.

Risks of Discrimination Claims and Lawsuits

Although this is a fast-developing area of the law, you should counsel employers that just because claims asserted may be based on novel technologies does not mean that the risk of such claims is theoretical.

For instance, consider two recent cases:

- **EEOC v. iTutorGroup, Inc., No. 1:22-cv-02565 (E.D.N.Y. Aug. 9, 2023).** The Equal Employment Opportunity Commission (EEOC) claimed that three online tutoring companies violated the ADEA because the AI program they used for hiring “automatically reject[ed] female applicants age 55 or older and male applicants age 60 or older” in violation of Title VII and the ADEA. iTutorGroup agreed to pay \$365,000 to the group of rejected applicants, as well as adopting anti-discrimination policies and conducting training.⁶
- **Derek Mobley v. Workday, Inc.** In this case, one of the first major class action lawsuits in this space, the plaintiff alleges that Workday’s applicant screening software unlawfully discriminated against job applicants based on race, age, and disability in violation of Title VII, the ADEA, and the ADA. Currently, the case is still pending, but as of the date of this article, it has survived two motions to dismiss.⁷

As more and more employers use more and more types of AI-assisted technology in various parts of the employment relationship, these types of lawsuits may only continue to proliferate. While all employment-related litigation presents risk, there are certain risks particular to claims associated with the use of AI, including the following:

- **Many potential plaintiffs.** The use of software such as that involved in the *iTutorGroup* and *Workday* cases affects many employees, quickly. Instead of just one individual hiring manager who might make unlawful decisions from time to time, or even one bad apple who intentionally makes such decisions individually, hundreds of employees may be impacted at once (and repeatedly) by decisions made by an algorithm.
- **Class action risk.** This means, too, that there is a higher risk of class action claims. Given their nature, disparate impact claims are more commonly brought as class actions. Class action litigation presents a host of risks for employers, as everything from discovery to potential settlement becomes more complicated and thus more expensive to manage.
- **Discovery challenges.** It is not always clear how AI tools make their decisions; as noted, algorithms can be a black

Related Content

For more information on how AI affects employment law and the workplace, see

 **ARTIFICIAL INTELLIGENCE: LAW AND LITIGATION § 6.01 ET SEQ.**

For an up-to-date tracker showing the progress of proposed or pending AI-related federal, state, and major local legislation across several practice areas, including Labor & Employment, see

 **ARTIFICIAL INTELLIGENCE LEGISLATION TRACKER (2024)**

For a comprehensive survey of enacted state and notable local AI legislation across several practice areas, including Labor & Employment, see

 **ARTIFICIAL INTELLIGENCE STATE LAW SURVEY**

To further explore diversity, equity, and inclusion (DEI) and employment discrimination legal issues, see

 **WORKPLACE DIVERSITY, LGBTQ, AND RACIAL AND SOCIAL JUSTICE RESOURCE KIT**

For a listing of materials on the legal issues concerning recruiting, screening, testing, hiring, and onboarding of new employees, see

 **SCREENING AND HIRING RESOURCE KIT**

box, so attempting to unravel their decision-making can be anything but straightforward. This means that audits or records supporting or explaining how an AI tool reached its decision may be difficult—or even impossible—to collect, review, preserve, or produce. This difficulty may be compounded by the fact that such tools are often third-party programs that are licensed by an employer. Unlike an individual hiring manager whose notes or records would be more likely to be readily available to their employer in the event of a lawsuit, third-party records may not be as readily available. Thus, even if electronic records exist for a given AI platform, an employer may face difficulty in securing data relevant to a claim that is not in the employer’s possession. All of this may add complexity to any AI-related claim and, likewise, increase the cost of defense.

⁶. See U.S. Equal Employment Opportunity Commission, *iTutorGroup to Pay \$365,000 to Settle EEOC Discriminatory Hiring Suit* (Sept. 11, 2023). ⁷. 2024 U.S. Dist. LEXIS 126336 (N.D. Cal. July 12, 2024).



Compliance with Myriad Federal, State, and Local Laws and Guidance

While a full analysis of all of the federal, state, and local laws and agency guidance governing the use of AI potentially relevant to employers is beyond the scope of this article, it is important for employers to be aware that in addition to laws prohibiting unlawful discrimination, there are myriad sources of legal guidance they should be aware of, including from agencies charged with enforcing anti-discrimination laws like the EEOC.

These include, but are not limited to:

Executive Agency Guidance

- President Biden’s Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence⁸
- The Equal Employment Opportunity Commission’s Guidance on Select Issues: Assessing Adverse Impact in Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures Under Title VII of the Civil Rights Act of 1964⁹

- The Department of Labor’s Artificial Intelligence and Worker Well-being: Principles for Developers and Employers¹⁰
- The Office of Federal Contract Compliance Programs’ Artificial Intelligence and Equal Employment Opportunity for Federal Contractors¹¹
- The National Labor Relations Board Memorandum Regarding Electronic Monitoring and Algorithmic Management of Employees Interfering with the Exercise of Section 7 Rights¹² and Memorandum of Understanding with Consumer Financial Protection Bureau¹³

State and Local Law

- The Illinois Artificial Intelligence Video Interview Act¹⁴
- The Maryland Facial Recognition Technology law¹⁵
- The New York City Automated Employment Decision Tools law¹⁶
- The Colorado Law Concerning Consumer Productions in Interactions with Artificial Intelligence Systems¹⁷

8. The White House, *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (Oct. 30, 2023) (rescinded January 20, 2025). 9. U.S. Equal Employment Opportunity Commission, *Select Issues: Assessing Adverse Impact in Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures Under Title VII of the Civil Rights Act of 1964* (May 18, 2023). 10. U.S. Department of Labor, *Artificial Intelligence and Worker Well-being: Principles and Best Practices for Developers and Employers*. 11. U.S. Office of Federal Contract Compliance Programs, *Artificial Intelligence and Equal Employment Opportunity for Federal Contractors* (Apr. 29, 2024). 12. National Labor Relations Board, Office of General Counsel, *Electronic Monitoring and Algorithmic Management of Employees Interfering with the Exercise of Section 7 Rights* (Oct. 31, 2022). 13. Consumer Financial Protection Bureau and National Labor Relations Board, *Memorandum of Understanding Between the Consumer Financial Protection Bureau and the National Labor Relations Board* (Mar. 7, 2023). 14. 820 Ill. Comp. Stat. Ann. 42/1. 15. Md. Code Ann., Crim. Proc. §§ 2-501 to -510. 16. N.Y. City Admin. Code §§ 20-870 to -874. 17. 2024 Bill Text CO S.B. 205.

You should consider the reliability of results made by algorithm in an AI-powered tool ... such programs are only as good as the data they are trained on and the human engineers who create them.

Ethical Considerations

Beyond compliance with anti-discrimination laws and guidance, employers should be aware that there are other traps for the unwary in the use of AI. This section addresses potential ethical or related concerns associated with the increased adoption of AI tools by employers.

Confidentiality and Privacy

As noted, AI tools aggregate huge amounts of data to make decisions. Sometimes, more data does not mean better decision-making. Some of this data should be kept confidential or may just be sensitive in nature. This could include information regarding medical conditions or treatment, employee leave, or performance or pay information that employees may not want shared, that should not be widely disseminated or that employers may not have traditionally relied on.

Lack of Reliability or Trustworthiness in Results

You should also consider the reliability of the results of decisions made by algorithm in an AI-powered tool. As noted above, such programs are only as good as the data they are trained on and the human engineers who create them. Thus, even if not unlawful, there exists the possibility of unfair results, results that cannot be satisfactorily unwound or explained, or even clear errors.

Failure to include at least some measure of human oversight may cause errors. For instance, an employer might not hire or promote a stellar candidate or employee who may have been a great fit because the candidate or employee did not meet pre-defined parameters or did not pass muster due to a glitch in video-interview software. Sometimes the best fit for a role may not look that way on paper, and a lack of human oversight means that individual may fall through the cracks.

Surveillance

With respect to AI tools that monitor employees, you should counsel employers to consider the ethical issues raised by employee surveillance. Even if such monitoring does not violate any applicable law (which should be confirmed) it’s important to consider culturally how employees may feel about

constant surveillance—and how that might translate into the workplace environment. Employers striving to create an inclusive culture that fosters belonging may find such efforts stymied by tools that make employees feel their every move is being watched and that they are not trusted.

Job Displacement and Skill Gaps

Separate from the risk of legal claims arising from specific employment actions or decisions lie more general risks that may arise more broadly from employers’ increased adoption of AI tools, including in how they conduct their day-to-day business.

As AI takes over more rote tasks, there is a risk that certain roles will be displaced. Some studies have shown that some of the roles most exposed to AI have been historically female-dominated (i.e., office or administrative support roles). Moreover, many employers are seeing an increased demand for individuals with skills in engineering or other STEM-related disciplines. Historically, at least, studies show that women and other minorities have been underrepresented in these roles.

Both trends thus have the potential to increase income inequality and decrease workplace diversity. Thus, you should counsel employers focused on DEI efforts to be aware of these potential risks and trends and make efforts to ensure upskilling and cross-training of their existing workforce and availability of open roles to a diverse pool of workers.





Practical Ways to Mitigate Risk

As described above, AI has many potential benefits and use cases. It also comes with uncertainty and risk. You should counsel employers seeking to use AI in a way to complement or supplement their DEI and anti-discrimination efforts (or, at least, avoid undermining them) to be aware of both. This section outlines practical steps you can share with employers to ensure they are getting the most of out of AI while avoiding potential pitfalls.

Adopt AI Thoughtfully

It's important for you to counsel employers to be deliberate and thoughtful in their adoption of AI-based tools. Advise employers to consider the following:

- **Comply with the law.** Identify and understand applicable guidance and laws governing AI as a threshold matter, to ensure that adoption and use of a given tool will not itself create risk. Ensure AI tools are not asking for or collecting information prohibited by law (for instance, about medical conditions or genetic information) or that could lead

to claims of discrimination (for instance, regarding an individual's age).

- **Create a task force.** Convene a task force to provide oversight on adoption and use of AI tools to ensure they are thoughtfully and consistently adopted, and make sure that the task force membership reflects diverse backgrounds, skillsets, and opinions. Consider similar diversity considerations in determining who at the employer will use AI tools.
- **Formalize a policy.** Draft a policy governing use of AI, both by employees and by the company. Establish clear ethical guidelines and rules for AI implementation and use.
- **Investigate vendors.** Ask vendors or partners offering or licensing AI tools about their testing efforts and how their algorithms are made and trained. Scrutinize the information provided to ensure, on the front end, that the tool will not result in underrepresentation of historically underrepresented groups.

- **Consider contractual protection.** If using a third-party tool, negotiate indemnification, warranty, and other risk-shifting language with vendors in the event of a claim raised in relation to a decision made by their technology. Negotiate up front the employer's ability to access underlying data in the event of such a claim, and the vendor's responsibility for protecting and retaining all such data confidentially.
- **Ensure diversity of teams and data.** If creating or customizing an AI-based tool in-house, be sure to put together a diverse team to provide input on its design and implementation. If using a vendor, ask about the makeup of the team involved in creating the product and where they sourced the underlying data used to train the algorithm.
- **Test and verify.** Engage in user testing of any AI tool to identify issues before formally implementing it more broadly.


Use AI Thoughtfully

Once an employer has implemented AI tools in the workforce, they must continue to be vigilant to ensure the tools are not creating risk or harming their progress toward DEI-related and anti-discrimination goals. You should advise employers to consider the following:

- **Prioritize human oversight.** Provide human checks and balances on AI tools. For instance, consider having a system in place to review candidates declined by an algorithm to ensure quality candidates are not being screened out, or that candidates who, for example, need an accommodation to complete AI-assisted screening processes are being given that opportunity. Be thoughtful in assessing job duties when feeding an AI tool job descriptions to screen candidates for.
- **Stay vigilant.** Continually reassess—perhaps with the assistance of the task force described above—whether AI tools are inadvertently harming historically underrepresented populations. Test and audit AI tools to identify potential bias. External vendors may be able to provide their own audits, and there are also numerous third-party testing tools available to perform audits to determine bias.
- **Provide notice.** Consider giving clear notice to employees and applicants that an AI tool will be used, even in places where such notice is not required by law. Consider including in addition to notice that AI will be used details about how it works and what qualifications are being assessed, and an opportunity to request a reasonable accommodation.
- **Protect sensitive information.** If using AI to conduct an audit, be mindful of what the results might reveal. Consider whether the scope may be narrowed and take steps to mitigate the risk of any sensitive findings, such as by



retaining counsel to oversee the audit to allow the result to be protected by attorney-client privilege, and by keeping the group involved in the project small and on a need-to-know basis.

- **Implement training.** Ensure that those using AI are trained on how to use it appropriately. And do not forget basic employment law compliance training. For instance, managers who use AI tools to assist in performance evaluation or management should be reminded of their obligations not to discriminate based on protected class, use of protected leave, or disability. And managers and AI vendors alike need to be reminded of their duty to recognize requests for accommodation. 

Emily Schifter is a partner at Troutman Pepper Locke. She handles a wide variety of labor and employment-related matters, including employment discrimination, leave, disability accommodation, and wage and hour litigation. Additionally, she counsels employers on many aspects of employment law and human resources issues.



RESEARCH PATH: [Labor & Employment](#) > [Screening and Hiring](#) > [Practice Notes](#)



Ellen M. Taylor SLOAN SAKAI YEUNG & WONG LLP

Examining the Application of Anti-Discrimination Laws to the Use of AI Technology

This article addresses the broad scope of artificial intelligence (AI) laws in the United States that focus on mitigating risk.

AI-DRIVEN EMPLOYMENT SCREENING SOFTWARE IS often marketed as a way to improve efficiency and eliminate or reduce bias by replacing the human element with automation. However, if it is not carefully designed, implemented, and monitored, this type of software can result in significant legal exposure for employers and vendors.

In *Mobley v. Workday*, a putative class action filed in the United States District Court for the Northern District of California, an employment applicant alleges that Workday, a human resources management platform, uses algorithmic and AI-driven job candidate-screening tools that resulted in unlawful discrimination against him and other job applicants on the basis of race, age, and disability.¹ Through this lawsuit, the plaintiff is seeking to represent not only himself, but numerous groups of individuals allegedly harmed by biases embedded into Workday's candidate-screening tools.² The class certification hearing in this action is scheduled for January 27, 2026.³ The conditional class certification hearing, which will occur before the final class certification hearing in this case, is scheduled to take place on April 8, 2025.

Although the plaintiff in this case has not named the employers that he applied to through Workday as defendants, the outcome of this case may impact employers who utilize AI-driven candidate-screening tools. If this case ultimately proceeds to trial and results in a finding that Workday is liable for violating anti-discrimination laws because its software adversely impacted individuals in protected classes, it is likely that some employers who use algorithmic candidate-screening tools will soon face class actions involving similar claims.

Plaintiff's Allegations

On February 21, 2023, Derek Mobley filed a putative class action complaint against Workday, a vendor that provides human resource management services, including algorithm-based applicant screening services, to thousands of companies, including numerous Fortune 500 firms.⁴ Mobley's initial complaint was dismissed with leave to amend,⁵ and he filed an Amended Complaint against Workday on February 20, 2024.⁶

In his First Amended Class Action Complaint (FAC), Mobley alleged that Workday violated Title VII of the Civil Rights Act of 1964,⁷ Section 1981 of Civil Rights Act of 1866,⁸ the Age Discrimination in Employment Act of 1967 (ADEA),⁹ the Americans with Disabilities

Act (ADA),¹⁰ and California's Fair Employment and Housing Act (FEHA),¹¹ because its artificial intelligence-driven algorithm screened out applications on the basis of race, age, and disability.¹²

According to the FAC, Workday provides "algorithmic decision-making tools" that "determine whether an employer should accept or reject an application for employment."¹³ Mobley alleged that Workday's tools "offer recommendations that reflect whatever biases employers happen to exhibit" and therefore "[cater] to the prejudicial preferences of the client-employer."¹⁴

Mobley claimed he applied for more than one hundred jobs through Workday,¹⁵ but all of his applications were rejected because the algorithm Workday was using to screen applicants dismissed his application on the basis that he is African-American, over the age of 40, and has a disability.¹⁶

Mobley allegedly applied to a wide range of companies through Workday, including medium and large global organizations that provide services in a variety of industries.¹⁷ He further claimed that he had been "qualified and in many instances overqualified" for the roles to which he applied.¹⁸ Mobley stated that he graduated with honors from the ITT Technical Institute, obtained a Server+ certification, and had worked in many information technology, financial, and customer service roles since 2010.¹⁹

Allegedly, Mobley's application process followed this pattern: he would click on a job advertisement on a third-party website and be redirected to a landing page on the employer's website featuring the Workday platform.²⁰ After that, Workday would prompt him to enter a username and password, and provided him the option of uploading a resume or typing in his information.²¹ Mobley alleged that his resume listed his graduation from a university that has a historically African-American student population, and it also listed his year of graduation, which could have been used as a proxy for his age.²²

Many of the applications that Mobley submitted through Workday allegedly required him to take a "Workday-branded assessment and/or personality test" that, while marketed as being "bias free," was designed to identify "mental health disorders or cognitive impairments" that have "no bearing on whether Mobley would be a successful employee."²³

¹ See First Amended Class Action Complaint (FAC), *Mobley v. Workday, Inc.*, No. 23-cv-00770-RFL (N.D. Cal. Feb. 20, 2024) at ¶¶ 49, 131, 140, 149, 154, 160, 170. ² FAC, *supra* note 1, at ¶ 8. ³ Case Schedule, *Mobley*, No. 23-cv-00770-RFL (Sept. 4, 2024). ⁴ *Mobley v. Workday, Inc.*, 2024 U.S. Dist. LEXIS 11573 (N.D. Cal. Jan. 19, 2024) at *4. ⁵ 2024 U.S. Dist. LEXIS 11573, at *3. ⁶ FAC, *supra* note 1. ⁷ 42 U.S.C.S. § 2000e et seq. ⁸ 42 U.S.C.S. § 1981. ⁹ 29 U.S.C.S. § 621 et seq. ¹⁰ 42 U.S.C.S. § 12101 et seq. ¹¹ Cal. Gov't Code § 12900 et seq. ¹² FAC, *supra* note 1, at ¶¶ 49, 131, 140, 149, 154, 160, 170. ¹³ FAC, *supra* note 1, at ¶ 28. ¹⁴ FAC, *supra* note 1, at ¶¶ 38-39. ¹⁵ FAC, *supra* note 1, at ¶¶ 131, 140, 149, 154, 160, 170. ¹⁶ FAC, *supra* note 1, at ¶¶ 131, 140, 149, 154, 160, 170. ¹⁷ FAC, *supra* note 1, at ¶ 89. ¹⁸ FAC, *supra* note 1, at ¶ 88. ¹⁹ FAC, *supra* note 1, at ¶¶ 24-25. ²⁰ FAC, *supra* note 1, at ¶¶ 51-53. ²¹ FAC, *supra* note 1, at ¶ 55. ²² FAC, *supra* note 1, at ¶ 55. ²³ FAC, *supra* note 1, at ¶¶ 56-57, 75.

Mobley claimed that he sometimes received rejections from jobs on the very same day that he applied to them through Workday.²⁴ On at least one occasion, Mobley was allegedly notified of a rejection less than one hour after he submitted his application.²⁵

Based on the foregoing, Mobley contended that Workday's algorithm discriminated against him and other job applicants who were over the age of 40, disabled, and/or African-American.²⁶ Mobley asserted federal law claims under Title VII, Section 1981, the ADEA, and the ADA for intentional discrimination on the basis of race and age, and disparate impact discrimination on the basis of race, age, and disability. Mobley claimed that Workday was liable for discrimination under Title VII, the ADEA, and the ADA as an employment agency and/or as an employer based on the theories that Workday was the agent of employers, and/or an indirect employer.²⁷

Mobley also asserted a claim against Workday for aiding and abetting its client-employers' to engage in unlawful race, disability, and age discrimination in violation of FEHA.²⁸

Workday’s Motion to Dismiss the FAC

On March 12, 2024, Workday filed a Motion to Dismiss the FAC, arguing, among other things, that as a software vendor, it is not a covered entity under Title VII, the ADEA, or the ADA and that an employer's agent cannot be held liable under the anti-discrimination statutes at issue for functions that the agent performs on the employer's behalf.²⁹

The EEOC’s Amicus Brief

On April 9, 2024, the Equal Employment Opportunity Commission (EEOC) submitted an Amicus Brief in opposition to the motion to dismiss.³⁰ The EEOC’s Amicus Brief argued that Mobley had alleged facts sufficient to support a reasonable inference that Workday is a covered entity under Title VII, the ADA, and the ADEA under the longstanding legal theories that Workday was an employment agency, an indirect employer, and/or an agent of its client-employers.³¹

24. FAC, *supra* note 1, at ¶¶ 76, 77, 85. 25. FAC, *supra* note 1, at ¶ 85. 26. FAC, *supra* note 1, at ¶¶ 131, 140, 149, 154, 160, 170. 27. Mobley v. Workday, Inc., 2024 U.S. Dist. LEXIS 126336 (N.D. Cal. July 12, 2024) at *7. 28. 2024 U.S. Dist. LEXIS 126336, at *5-6. 29. 2024 U.S. Dist. LEXIS 126336, at *9. 30. Brief of the Equal Employment Opportunity Commission as Amicus Curiae, Mobley, No. 23-cv-00770-RFL (N.D. Cal. April 9, 2024). 31. EEOC Amicus Brief, *supra* note 30, at 8.



Related Content

For a presentation on environmental, social, and corporate governance employment law issues, see

 **ENVIRONMENTAL, SOCIAL, AND GOVERNANCE (ESG) FOR EMPLOYERS AND HR: TRAINING PRESENTATION**

For more resources on artificial intelligence (AI), see

 **GENERATIVE ARTIFICIAL INTELLIGENCE (AI) RESOURCE KIT**

For a primer on the key issues relating to employment discrimination and diversity, equity, and inclusion (DEI) when using AI tools, see

 **AI AND DEI & EMPLOYMENT DISCRIMINATION: KEY LEGAL ISSUES AND POTENTIAL PITFALLS & BENEFITS**

For guidance and best practices for counseling employers on legal implications of AI in the workplace, see

 **ARTIFICIAL INTELLIGENCE IN THE WORKPLACE: BEST PRACTICES**

For an analysis of the potential legal and business risks stemming from the use of AI tools to manage employee performance and make employment decisions, see

 **AI IN EMPLOYMENT DECISIONS AND PERFORMANCE MANAGEMENT: KEY LEGAL ISSUES AND POTENTIAL RISKS AND BENEFITS**

For PowerPoint slides on how AI is impacting employment law and the workplace, see

 **AI IN THE WORKPLACE: HOW AI IS IMPACTING EMPLOYMENT LAW TRAINING PRESENTATION**

For a video examining key considerations regarding AI in the workplace, see

 **ARTIFICIAL INTELLIGENCE (AI) IN THE WORKPLACE VIDEO**

For an in-depth listing of key federal litigation concerning AI labor and employment, generative AI, and AI copyright infringement and registrability issues, see

 **ARTIFICIAL INTELLIGENCE: FEDERAL LITIGATION TRACKER**

The Court’s Order Denying in Part and Granting in Part Workday’s Motion to Dismiss

On July 12, 2024, the district court denied Workday’s motion to dismiss in part and granted it in part (Order).³²

The court first analyzed whether Workday was a covered entity under the anti-discrimination statutes based on any of the theories asserted by Mobley. The court held that Mobley could not proceed on a theory that Workday could be held liable as an employment agency because he failed to allege facts sufficient to infer that Workday regularly “finds employees for employers.”³³ Accordingly, to the extent that Mobley’s Title VII, ADEA, and ADA claims were based on an employment agency theory of liability, the motion to dismiss was granted.³⁴

However, the court noted that liability as an employment agency and liability as the agent of an employer are not “coextensive.”³⁵ Here, the court determined that because Mobley sufficiently alleged that Workday functions as an agent for employers by determining which candidates are rejected or obtain interviews, Workday “falls under the definition of an ‘employer’ under Title VII, the ADEA, and ADA” and may be liable under those statutes.³⁶ The court did not reach Mobley’s alternative argument that Workday is an employer under an indirect employer theory.³⁷

Because Mobley sufficiently pleaded that Workday was a covered entity, the court next analyzed whether Mobley sufficiently alleged disparate impact and intentional discrimination claims under the federal anti-discrimination statutes. With respect to Mobley’s disparate impact claims under Title VII, the ADEA, and the ADA, the court denied Workday’s motion, finding that from the facts alleged, it could plausibly be inferred that there was a disparate impact on applicants with Mobley’s protected traits that was caused by Workday’s algorithmic selection tools.³⁸ However, the court granted Workday’s motion and dismissed Mobley’s intentional discrimination claims under Title VII, the ADEA, and Section 1981 without leave to amend, holding that Mobley had not sufficiently alleged that Workday “intended its screening tools to be discriminatory.”³⁹

Finally, because Mobley failed to allege that any specific company discriminated against him or that Workday knew that any of its client-employers’ conduct was discriminatory, the court dismissed Mobley’s aiding and abetting claim under FEHA with leave to amend.⁴⁰

Although Mobley has named only Workday as a defendant and not the employers to which he applied through the Workday platform, the court’s Order makes it clear that the outcome of this case will likely impact employers who use AI employment screening tools.

32. 2024 U.S. Dist. LEXIS 126336, at *32-33. 33. 2024 U.S. Dist. LEXIS 126336, at *10-12. 34. 2024 U.S. Dist. LEXIS 126336, at *19-22. 35. 2024 U.S. Dist. LEXIS 126336, at *11. 36. 2024 U.S. Dist. LEXIS 126336, at *19. 37. *Id.* 38. 2024 U.S. Dist. LEXIS 126336, at *25. 39. 2024 U.S. Dist. LEXIS 126336, at *28. 40. 2024 U.S. Dist. LEXIS 126336, at *31.



Specifically, the Order elucidates the court’s position that although Title VII, the ADEA, and ADA may predate some AI-powered job candidate-screening platforms, the use of these platforms in a manner that results in a disparate impact to members of classes protected under these statutes could still subject developers and employers to liability.

As the Workday platform is allegedly the gatekeeper that determines whether a job candidate will be interviewed for a position with the employer, the court asserted that Workday’s platform is “engaged in conduct that is at the heart of equal access to employment opportunities.”⁴¹ Failing to recognize possible agency liability for third-party developers who engage in such conduct “would allow companies to escape liability for hiring decisions by saying that function has been handed over to someone else (or here, artificial intelligence)” and would “cut[] against the well-recognized directive that courts are to construe remedial statutes such as Title VII, the ADEA, and the ADA broadly to effectuate their purposes.”⁴²

The court explained that “[n]othing in the language of the federal anti-discrimination statutes or the case law interpreting those statutes distinguishes between delegating functions to an automated agent versus a live human one.”⁴³ The court further pointed out that “[d]rawing an artificial distinction between software

Related Content

For an up-to-date tracker showing the progress of proposed or pending AI-related federal, state, and major local legislation across several practice areas, including Labor & Employment, see

 [ARTIFICIAL INTELLIGENCE LEGISLATION TRACKER \(2024\)](#)

For a comprehensive survey of enacted state and notable local AI legislation across several practice areas, including Labor & Employment, see

 [ARTIFICIAL INTELLIGENCE STATE LAW SURVEY](#)

To further explore DEI and employment discrimination legal issues, see


 [WORKPLACE DIVERSITY, LGBTQ, AND RACIAL AND SOCIAL JUSTICE RESOURCE KIT](#)

For a listing of materials on the legal issues concerning recruiting, screening, testing, hiring, and onboarding of new employees, see

 [SCREENING AND HIRING RESOURCE KIT](#)

decisionmakers and human decisionmakers would potentially gut anti-discrimination laws in the modern era,”⁴⁴ because it would allow employers to “delegat[e] discriminatory programs to third-party software tools, with job applicants and employees having little recourse to challenge such discrimination.”⁴⁵

Takeaway

The widespread use of robust, AI-driven job candidate-screening tools is still a relatively new development, and the legal framework regulating employers’ use of AI in the workplace is still evolving. However, the court’s rationale in this Order highlights the exposure employers may face if they utilize AI-driven screening software that has a disparate impact on members of protected classes under law. 

Ellen M. Taylor is Senior Counsel at Sloan Sakai Yeung & Wong LLP, where she represents employers in labor, employment, and government law matters. She can be reached at etaylor@sloansakai.com.

⁴¹. 2024 U.S. Dist. LEXIS 126336, at *16. ⁴². 2024 U.S. Dist. LEXIS 126336, at *14 (citing *Moyo v. Gomez*, 40 F.3d 982 (9th Cir. 1994)). ⁴³. 2024 U.S. Dist. LEXIS 126336, at *16. ⁴⁴. 2024 U.S. Dist. LEXIS 126336, at *17. ⁴⁵. 2024 U.S. Dist. LEXIS 126336, at *18 (quoting *City of L.A. Dep’t of Water & Power v. Manhart*, 435 U.S. 702, 718 n.33 (1978)).

This article was originally published in [Bender’s California Labor & Employment Bulletin, 2024-11 Bender’s California Labor & Employment 01 \(2024\)](#).

WHAT’S NEW

Practical Guidance

Learn About New Practical Guidance Content and Resources

Review this exciting guide to some of the recent content additions to Practical Guidance, designed to help you find the tools and insights you need to work more efficiently and effectively. **Practical Guidance customers, please follow this link.**

Not a Practical Guidance Subscriber? [Sign up for a FREE seven-day trial here](#) to access the featured content in this guide.

Highlights include:

- **Environmental, Social, and Governance (ESG) for Employers and HR: Training Presentation:** This presentation is designed for employers and HR professionals in the U.S. and the UK. It explains what ESG is and how it affects employers and the work of HR professionals. Employers should adapt and customize this presentation to focus on the ESG issues that are most important for their organizations.
- **AI in the Workplace: How AI is Impacting Employment Law Training Presentation:**
 - This presentation by Eric Dreiband and Mary Katherine “Kassie” Callesen, Jones Day, provides guidance on how artificial intelligence (AI) is impacting employment law and the workplace.
- **AI Drafting Company Artificial Intelligence Policies:**
 - This practice note, by Eric Felsberg and Douglas Klein, Jackson Lewis P.C., provides guidance to employers when creating artificial intelligence (AI) policies in the workplace
- **New AI-Related Hot Topic Practice Notes**
 - [What Lawyers Need to Know about Deepfake Technology](#), offering:
 - Guidance on deepfake creation and detection technologies –and–
 - Best practices for dealing with deepfakes in litigation, including preserving corroborating evidence.
 - **Deepfakes and the Federal Rules of Evidence: How to Challenge Authenticity and Admissibility:** guides attorneys on how to attack potential deepfake evidence in federal court, including:
 - Challenging authenticity
 - Seeking sanctions for deepfake use





Jessica Bishop and Sarah Stothart GOODMANS LLP

Artificial Intelligence (AI) Agreements Checklist

This checklist provides an overview of key legal considerations attorneys should review when advising clients on negotiating and drafting contracts involving artificial intelligence (AI). Considerations may vary depending on the jurisdiction and nature of the AI at issue.

1. Define the Scope of Work and Deliverables

- As with any technology contract, clearly define and describe the scope of services and deliverables in the contract.
- Consider and review whether the AI product description, documentation, specifications, deliverables, and contractual terms meet the client's requirements.

2. Address Intellectual Property (IP) Ownership

- The contract should address IP ownership between the parties with respect to:
 - ✓ The deliverables
 - ✓ The AI
 - ✓ All input and output
 - ✓ Any training data
- If the customer provides inputs or prompts to the AI solution, the customer may wish to continue to own the inputs or prompts. Also consider whether the customer would expect any ownership rights in the output, including any deliverable created from that output.
- Prompts and certain customer data may include information that the vendor expects or requires the right to use and to allow third parties to use. The vendor should include provisions protecting its:
 - ✓ Rights in the AI
 - ✓ Vendor information and data
 - ✓ Trade secrets
 - ✓ Copyrighted materials
 - ✓ Patents or patent applications

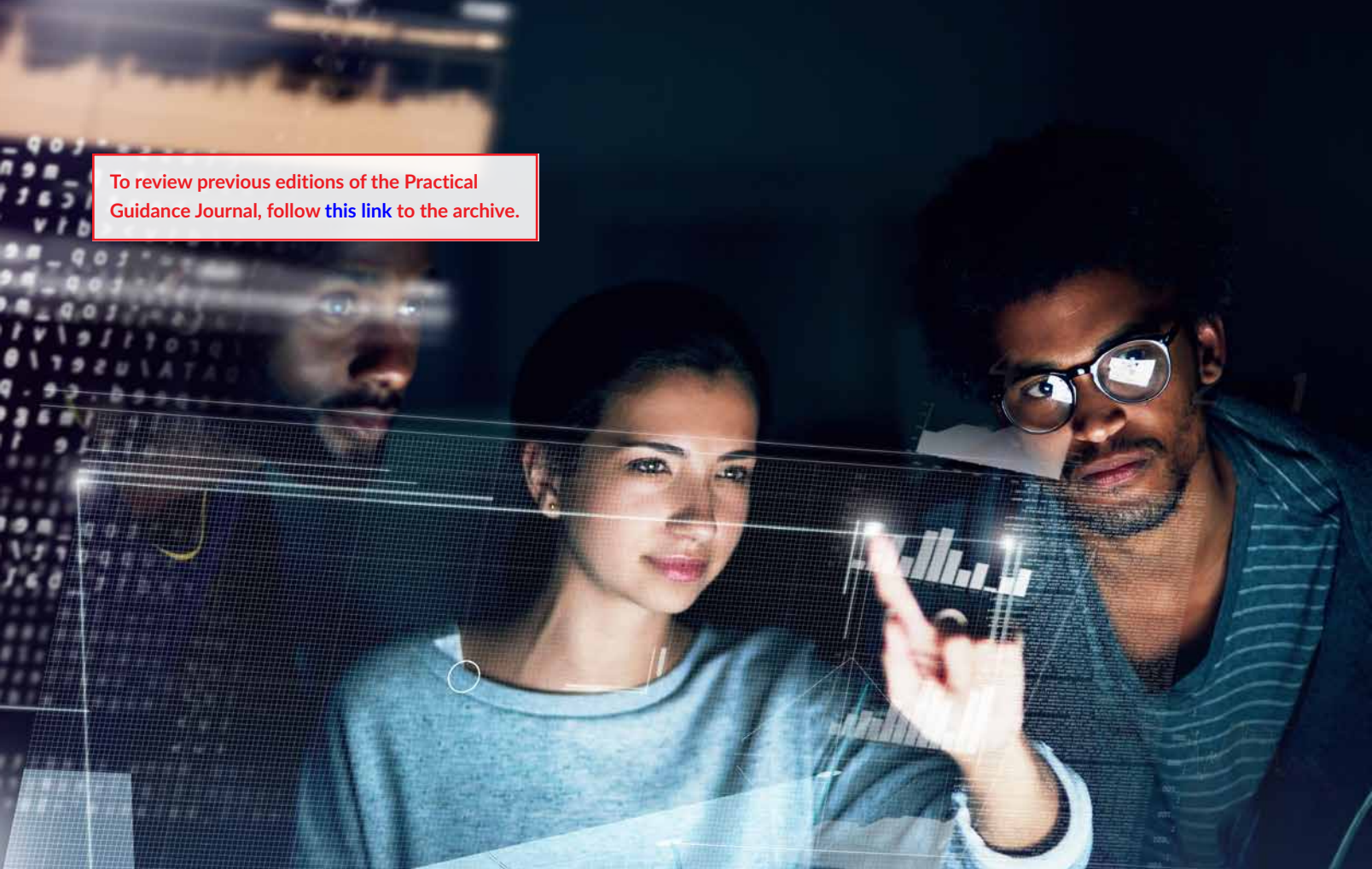
- Factor these requirements into the definition of the deliverables and corresponding ownership and use rights.
- AI solutions often rely on the use of open-source software and third-party software. Consider whether open-source software or third-party software will be incorporated into any deliverables or services and any associated IP or data security risks.
- In many cases, contracting parties may choose to maintain secrecy over components of the AI. Contracting parties should maintain awareness of applicable trade secrets legislation and should include strict confidentiality provisions in contracts, specifying that a breach would result in irreparable harm that is not compensable in damages.
- In connection with the foregoing considerations of ownership of applicable property, consider and provide for any necessary licenses over such property. Licenses may be limited to the duration of the contract period but no longer or may vary depending on the purpose to which the AI is put.

3. Include Performance and Service Levels

- As with any technology contract, a contract for an AI solution should contain robust performance and quality metrics that reflect the customer's requirements. If the vendor or its subcontractor is hosting the AI, standard service levels for availability of the AI should be included in the contract.
- Service level requirements should be included for any customer requirements relating to items such as incidents, support, and processing times, as well as service level objectives for items that require tracking and reporting.
- Where AI solutions will be used as workplace tools by regulated industries or by clients with professional obligations, ensure that the contract allows the client and any users to comply with all:
 - ✓ Regulations
 - ✓ Professional obligations
 - ✓ Policies



To review previous editions of the Practical Guidance Journal, follow [this link](#) to the archive.



4. Draft Representations and Warranties

- Customers should require vendors to represent and warrant that:
 - ✓ Vendor has all the necessary rights and licenses to use any third-party and open-source technology to provide the AI solution, deliverables, and any services.
 - ✓ Vendor has full power and authority to grant the rights to the customer under the contract.
 - ✓ The AI solution, deliverables, and any services will not misappropriate, violate, or infringe any third-party IP rights (this is in addition to indemnification protection for third-party IP claims).
 - ✓ The vendor and its AI solution, services, and deliverables will comply with all specifications and all applicable laws, including all privacy laws.
- Potential weaknesses of AI solutions include bias and data quality. If representing a customer, consider including representations and warranties that mitigate the risks associated with bias (if applicable to the AI solution) and data quality.
- If representing a vendor, consider the use of disclaimers with respect to limitations and risks of the AI solution. Errors in outputs could result from customer prompts or bad input data.
- Vendor should require customers to represent and warrant that:
 - ✓ The customer and its use of the AI solution and services will comply with all applicable laws.
 - ✓ The customer has all necessary rights and consents required to allow the vendor to process its data, including all personal information, in accordance with the contract.

5. Consider Data Privacy

- Organizations should prudently determine if the AI solution will process personal information. When making this determination, each type of data, including the input data, output data, and any training data should be considered. Also consider whether the output data could constitute newly generated personal information.
- AI solutions typically involve the processing of large volumes of data that may contain personal information.
- The organization providing the personal information to be processed, and in some cases, the processor as well, is responsible for ensuring that the necessary consent has been obtained for the processing of personal information by the AI.
- Robust data-protection terms should be included in the contract to ensure compliance with all applicable privacy laws, including health privacy laws where personal health information is processed, and to restrict the use of personal information. The data-protection terms should expressly limit the use of personal information to the purposes for which consent has been provided.
- Personal information should be defined in a manner consistent with applicable privacy laws. Under U.S. law, the definition of personal information varies by jurisdiction. The Canadian courts have determined that the definition of personal information is usually to be given a broad and expansive interpretation (e.g., information will be personal information if it is about an identifiable individual. A person will be identifiable if the information disclosed, together with other publicly available information, would tend to or possibly identify them).

6. Consider Security

- The security of AI solutions is a key consideration, particularly when processing data that may contain personal information, or sensitive or otherwise confidential information. AI solutions can present potential cybersecurity risks that threat actors can attempt to exploit by compromising the security of the system or obtaining confidential data.
- Organizations that collect, use, and disclose personal information are obliged to establish physical, technical, and organizational safeguards appropriate to the sensitivity of the information. Those safeguards must protect against risks such as loss or theft, unauthorized access, disclosure, copying, use, or modification.
- AI solutions raise the same security concerns as other software, with a few specific considerations:
 - ✓ Some AI solutions access large datasets which can heighten the risks associated with data breaches, and breach-related incidents can be difficult to reconstruct.
 - ✓ AI processes may be proprietary or opaque, which makes it difficult to determine whether the AI system is processing data in accordance with the contract or whether it has been tampered with.
 - ✓ Allowing training data or outputs to be accessed or used in a manner that is not authorized is a risk.
 - ✓ The possibility of re-identification of data with individuals arising from the architecture of AI systems and output is a risk.
- Customer-specific considerations:
 - ✓ Customers should understand the AI solution architecture and any security vulnerabilities to enable them to better mitigate risks and bolster cybersecurity programs and policies.
 - ✓ Customers should ask for security-related specifications and requirements and such terms should be included in the contract.
- Vendor-specific considerations:
 - ✓ Vendors should consider adding security-related disclaimers making it clear that the AI solution is not free from third-party interference or otherwise secure.
 - ✓ Vendors may want to require customers to follow security practices to address risks stemming from the customer's systems and access to the AI solution and to require customers to protect the integrity and security of input data and training data (if provided by customer).

7. Consider Risk Management and Liability

- Evaluate the risk/benefit of the AI system:
 - ✓ Before entering the contract, consider all of the following:
 - The specific use case for the AI
 - Its historical performance
 - Whether it is being implemented for a high-risk function
 - ✓ Depending on these factors, consider whether the benefit of implementation is sufficient to warrant the outsourcing of performance to an AI system with the associated uncertainty and risk that may be incurred.
- Responsibility for issues/performance failures:
 - ✓ The contract should clearly set out the allocation of liability for any resulting issue, including harm to the parties and third parties when an AI system results in error or incurs liability.
 - ✓ The negotiated allocation of responsibility for resulting issues may depend on the source of the issue and the negotiated allocation of responsibility (e.g., development or maintenance of the AI).
- Performance oversight:
 - ✓ The contract should specifically allocate responsibility for performance oversight. This should include:
 - Development of contractual agreement to the implementation of safety mechanisms
 - Procedures and the conduct of regular auditing and testing
 - ✓ The AI must perform in compliance with the parties' own performance requirements, but, depending on the context, the AI may also be required to comply with third-party expectations of performance.
- Third-party terms of use:
 - ✓ To the extent the subject AI will be accessed or used—directly or indirectly—by third parties, stipulate terms of use that bind such third-party usage. Terms of use will need to be publicly posted for agreement by third parties at the time of use.
 - ✓ Carve-outs can be documented in the main contract to specify where liability is subject to third-party terms of use.
- Documentation and Recordkeeping:
 - ✓ The parties should ensure that all aspects of development and deployment of the AI system are documented.
 - ✓ When problems with an AI system arise, one of the most important factors in being able to resolve and correct them is a transparent and well-documented system where the source of the issue is identifiable.
 - ✓ Documentation and recordkeeping obligations—and consequences for failure to comply—should be specified in the contract.



8. Address Indemnification

- Related to the foregoing risk management considerations, contracting parties should agree to appropriate indemnification provisions that are consistent with the allocation of responsibility and liability discussed above.
- Indemnification should address direct and consequential harms, harms to third parties, and allegations of IP infringement.

9. Understand Ethical Considerations

- Depending on the purpose to which the subject AI will be put, ensure multi-stage controls are in place to evaluate and ensure performance complies with applicable human rights and discrimination legislation, as well as company policies.

10. Comply with Legal and Regulatory Requirements

- Regularly review and ensure compliance with all local statutory, common law, and regulatory requirements. Different jurisdictions are introducing new legal requirements regularly addressing AI-specific issues (e.g., EU AI Act, Colorado AI Act). Contracts should ensure compliance with any such laws but also provide for regular updates to capture any subsequently developed laws.
- Contracting parties must also comply with industry-specific laws.
- Depending on the jurisdiction, parties should recognize that contractual performance is often subject to an overarching duty of good faith and honest performance that may require honest and good faith exercise of any discretionary entitlements under the contract or any termination provisions, for example.

Related Content

For an in-depth discussion of indemnification, see

 [INDEMNIFICATION PROVISIONS IN COMMERCIAL CONTRACTS](#)

For updates on state, federal, and municipal legislation related to the use of Artificial Intelligence (AI), see

 [ARTIFICIAL INTELLIGENCE LEGISLATION TRACKER \(2024\)](#)

For a full listing of practical guidance materials on generative AI, ChatGPT, and similar tools across multiple practice areas, see

 [GENERATIVE ARTIFICIAL INTELLIGENCE \(AI\) RESOURCE KIT](#)

For further discussion of service levels, see

 [SOFTWARE AND IT SUPPORT AGREEMENTS: SERVICE LEVELS](#)

For an examination of dispute resolution and remedies in outsourcing transactions, see

 [DISPUTE RESOLUTION AND REMEDIES IN OUTSOURCING](#)

For an overview of data security and privacy, see

 [PRIVACY AND DATA SECURITY CONSIDERATIONS WHEN NEGOTIATING OR REVIEWING A TRANSACTION OR AGREEMENT](#)





Related Content

For a summary of key federal litigation related to AI, see

 **ARTIFICIAL INTELLIGENCE: FEDERAL LITIGATION TRACKER**

To track recent guidance, decisions, and actions taken by the U.S. Patent and Trademark Office and the U.S. Copyright Office related to AI, see

 **ARTIFICIAL INTELLIGENCE: INTELLECTUAL PROPERTY REGULATORY TRACKER**

For a look at the primary and emerging legal issues related to AI, see

 **ARTIFICIAL INTELLIGENCE KEY LEGAL ISSUES**

For a presentation on environmental, social, and corporate governance employment law issues, see

 **ENVIRONMENTAL, SOCIAL, AND GOVERNANCE (ESG) FOR EMPLOYERS AND HR: TRAINING PRESENTATION**

For information on key AI-related considerations in mergers and acquisitions due diligence, see

 **ARTIFICIAL INTELLIGENCE (AI) INVESTMENT: RISKS, DUE DILIGENCE, AND MITIGATION STRATEGIES**

11. Provide for Dispute Resolution

■ Establish mechanisms for dispute resolution:

- ✓ Executive negotiation
- ✓ Third-party mediation
- ✓ Private arbitration
- ✓ Litigation

■ Provide for any desired time periods or requirements to be met prior to any subsequent dispute resolution step.

■ Specify the jurisdiction in which resolution is to occur and the law which will govern any disputes.

Jessica Bishop is a partner in a business law group at Goodmans. Her practice focuses on corporate and commercial law with a focus on complex commercial technology transactions.

Sarah Stothart is a partner in the litigation and dispute resolution group at Goodmans. She maintains a broad practice primarily divided between complex commercial, insolvency, and intellectual property litigation.

 **RESEARCH PATH:** [Intellectual Property & Technology >](#)
[IP & IT in Corporate Transactions >](#) [Checklists](#)

Welcome to what comes next.

Lexis+ AI returns trusted results backed by verifiable authority 2X faster than Westlaw®, enabling you to work more efficiently than ever.

Transform your legal work

LEARN MORE: [LEXISNEXIS.COM/AI](https://www.lexisnexis.com/ai)

Innocence Canada Seeks Justice for Wrongly Convicted, Works to Prevent Further Cases



Those seeking assistance from Innocence Canada must meet two eligibility criteria: wrongful conviction of a homicide offense and unsuccessful appeal of the conviction to a provincial court of appeal or the Supreme Court of Canada. Case review by staff attorneys and volunteer lawyers takes several years. Only those cases which reveal new evidence or information are considered for further investigation.

A registered charitable organization, Innocence Canada relies heavily on donations to cover expenses such as private investigators, forensic testing, expert witnesses, court fees, travel costs, and transcripts of proceedings.

Members of the LexisNexis Canada content team in Toronto recently took part in a RELX Cares charity walk to support Innocence Canada, raising \$1250 in donations from both office-based and home-based employees. RELX Cares supports employee and corporate engagement that makes a positive impact on society through volunteerism and giving, including efforts that support the rule of law. As part of its commitment to volunteerism, LexisNexis provides two paid volunteer days to employees each year.

LexisNexis supports the rule of law around the world by:

- Providing products and services that enable customers to excel in the practice and business of law and help justice systems, governments, and businesses to function more effectively, efficiently, and transparently



- Documenting local, national and international laws and making them accessible in print and online to individuals and professionals in the public and private sectors
- Partnering with governments and non-profit organizations to help make justice systems more efficient and transparent and
- Supporting corporate citizenship initiatives that strengthen civil society and the rule of law across the globe.

For more information on Innocence Canada, visit www.innocencecanada.com.

Since its founding in 1993, Innocence Canada, a non-profit based in Toronto, has helped to exonerate 30 innocent people who were wrongfully convicted of murder. The group's mission is "to identify, advocate for and support the exoneration of individuals who have been convicted of a crime they did not commit and to prevent wrongful convictions through legal education, advocacy, and justice reform."

IN THE MOST RECENT CASE, TWO MEN, BOBBY MAILMAN and Wally Gillespie, had their convictions overturned in January 2024, 40 years after their imprisonment for a 1983 murder they did not commit. Both men were sentenced to life in prison by a New Brunswick court, despite statements from multiple witnesses placing them miles from the murder scene. Attorneys at Innocence Canada worked on the case for six years, arguing that the prosecution had wrongfully failed to provide the defense with critical evidence that could have changed the outcome of the case. In addition to the exoneration, the two men received an undisclosed

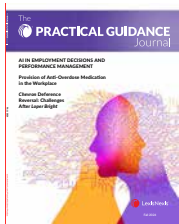


amount in compensation from the New Brunswick government. Gillespie passed away several months later at the age of 80. Mailman, who is 77, has been diagnosed with terminal cancer.

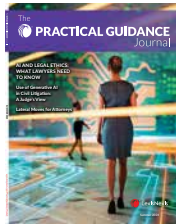


Practical Guidance Journal Archive

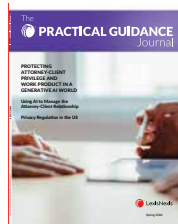
Browse the complete collection of Journals



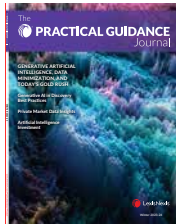
Fall 2024



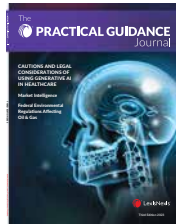
Summer 2024



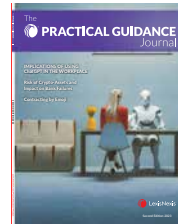
Spring 2024



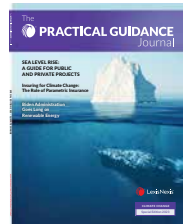
Winter 2023-24



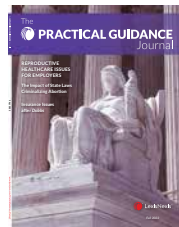
Third Edition 2023



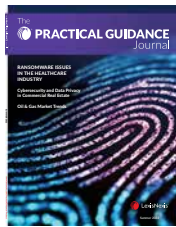
Second Edition 2023



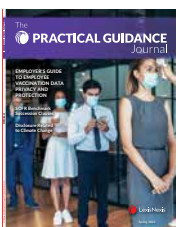
Special Edition:
Climate Change



Fall 2022



Summer 2022



Spring 2022



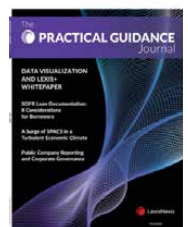
Fall 2021



Summer 2021



Spring 2021



Fall 2020



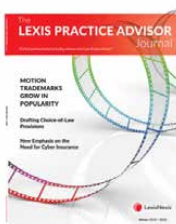
Summer 2020



Special Edition:
Coronavirus



Spring 2020



Winter 2019 / 2020



Special Edition:
Energy & Utilities



Fall 2019



Summer 2019



Special Edition: Healthcare
Practice



Spring 2019



Winter 2018



Special Edition:
Civil Litigation



Fall 2018



Summer 2018



Special Edition:
Labor & Employment



Spring 2018



December 2017



Special Edition:
Corporate Counsel



Fall 2017



Summer 2017



Spring 2017



Winter 2017



Special Edition: Privacy & Data
Protection



Fall 2016



Special Edition: Finance



Summer 2016



Spring 2016



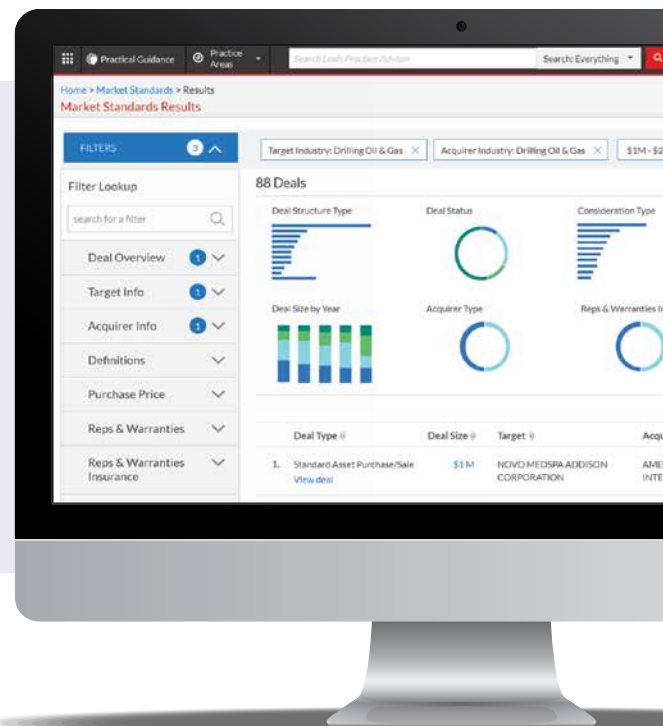
Winter 2015/16

MARKET STANDARDS

Search, Compare, Analyze
More Public M&A Deals

Data-Driven Practical Guidance for M&A Attorneys

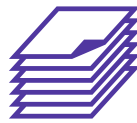
Market Standards helps M&A attorneys search and compare transactions using highly negotiated deal points, easily find precedent language, and see deal point and transactional trends with data visualizations.



COMPARED TO OTHER OFFERINGS*



33,000 deals
(6x more)



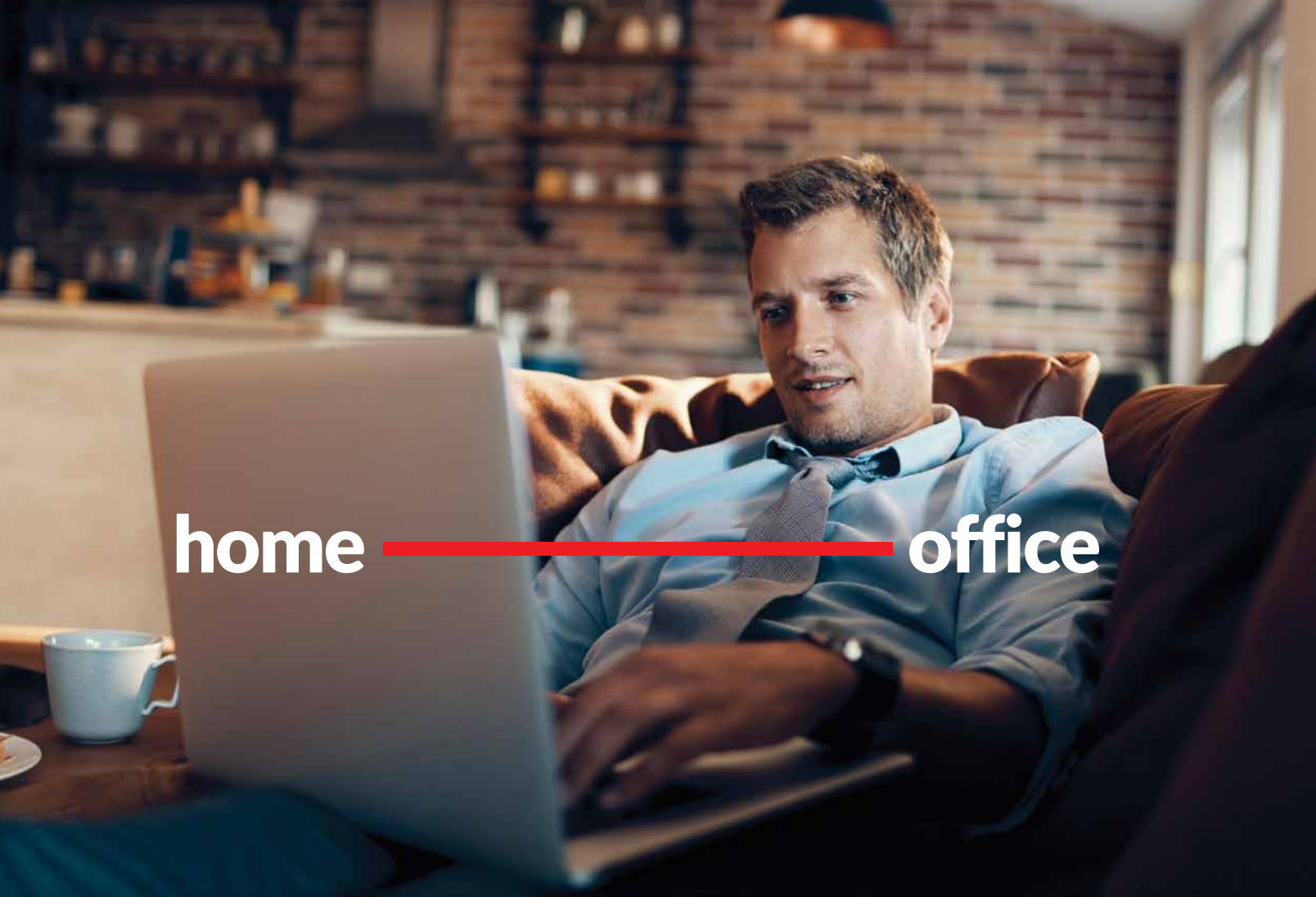
150 deal points
(2x more detail)



Sec updates within
48 hours (3x faster)

See how Market Standards can boost your efficiency
and give you an edge in your M&A deals.

[LexisNexis.com/LexisPracticalGuidance](https://www.lexisnexis.com/LexisPracticalGuidance) | Call us today at 800.628.3612.



home — office

**Always connected
legal eBook research
for wherever your
work happens.**



Read easily in a web browser or in your preferred eReader.



Search for terms, add notes, highlights and bookmarks for more personalized work productivity.



Link to the Lexis+™ and Lexis® services for deeper online access to law sources.*

LexisNexis® eBooks

SHOP FOR LEGAL EBOOKS AT lexisnexis.com/eReading
CALL 800.223.1940

*Linking to the Lexis+ or Lexis service may not be available in all titles.
Access to the Lexis+ or Lexis service requires an active subscription.

LexisNexis, Lexis Advance and the Knowledge Burst logo are registered trademarks of RELX Inc.
Other products or services may be trademarks or registered trademarks of their respective companies. © 2021 LexisNexis. OFF04812-0 0221

