The 2025 General Counsel Toolkit Conference

AI in the Workplace: Legal Implications for Employers

June 10, 2025

ACC Association of Corporate Counsel NEW YORK CITY

JacksonLewis

XPO

Presenters

Eric J. Felsberg

Principal, Jackson Lewis P.C.

Eric.Felsberg@jacksonlewis.com

631.247.4640

Damon W. Silver

Principal, Jackson Lewis P.C.

Damon.Silver@jacksonlewis.com

212-545-4063

Rachel Ginsburg

Vice President, Labor and Employment Counsel,. XPO Logistics, Inc.

Rachel.Ginsburg@xpo.com

203-423-2088

Eric J. Felsberg

Eric J. Felsberg is a principal in the Long Island, New York office of Jackson Lewis P.C. and co-leader of the firm's Artificial Intelligence and Technology Groups. An early adopter, Eric has long understood the intersection of law and technology and the influence artificial intelligence has on employers today and will have on the workforce of the future.

Recognized as a leading voice in the industry, Eric monitors laws, regulations and trends, providing practical advice and answers to emerging workplace issues before his clients even know to ask the questions. He partners with clients to develop AI governance models, and provides advice and counsel on AI use policies, ethics and transparency issues related to AI products, systems and services. Eric leverages his considerable knowledge of the technology and AI industries to create meaningful partnerships with developers and distributors of AI models and tools and owners of content and data used to train AI applications for the benefit of his clients.

Damon W. Silver

Damon W. Silver is a principal in the New York City, New York, office of Jackson Lewis P.C. and co-leader of the firm's Privacy, Data and Cybersecurity practice group. He is also a Certified Information Privacy Professional (CIPP/US).

As a strategic advisor to local, regional, and national clients in various industries, Damon recognizes the demands of today's business climate and the ongoing threats that organizations face from cyberattacks, increased data privacy and security regulation, and the rapid integration of AI and other technologies in workplaces and workflows. Clients routinely seek Damon's guidance on how best to manage the day-to-day data privacy and security risks that arise when they engage in activities like monitoring of employee or customer activity; utilizing biometric information – like fingerprints or facial scans – for security or timekeeping purposes, or in connection with product offerings; leveraging data-based tools and strategies to pursue advertising and marketing objectives; and using AI chatbots and meeting assistants to transcribe meetings, draft emails, pull data, and make decisions about which customers to work with or applicants to hire.

Rachel Ginsburg

Rachel Ginsburg is Vice President, Labor and Employment Counsel at XPO, Inc. (f/k/a XPO Logistics), a global provider of transportation solution services headquartered in Greenwich, Connecticut. Rachel has been with XPO since 2018 and has led the Company through two spin-offs and a sale of one of its business units. Prior to joining XPO, Rachel was an attorney at Pullman & Comley, LLC, where she specialized in employment litigation defense.

Disclaimer

The presenters have prepared the materials contained in this presentation for the participants' reference and general information in connection with education seminars. Attendees should consult with counsel before taking any actions that could affect their legal rights and should not consider these materials or discussions about these materials to be legal or other advice regarding any specific matter.

What is AI?

JacksonLewis

Traditional AI v. Generative AI

Traditional AI

- Focuses on performing a specific task
- System designed to respond to a particular set of inputs
- System has the capacity to learn from data and make predictions based off that data
- Primarily used to analyze data and make predictions

Generative AI

- System has ability to create something new
- System is trained on a set of data and learns the underlying patterns
- Consider Chat GPT, Open AI's language prediction model
  - Trained on the internet, it can produce human-like test that is (almost) indistinguishable from text written by a human
- Primarily used to create new data similar to its training

Types of Machine Learning-Driven Hiring Tools

- **Resume Scanners:** filters or prioritize applicants using certain keywords.
- **Video Interviewing Software:** evaluate candidates based on their facial expressions, speech patterns and responses to job related questions.
- **“Virtual assistants” or “chatbots”:** ask candidates about their qualifications and reject those who do not meet the pre-defined requirements;
- **Testing software** – provides “job fit” scores for applicants regarding their personalities, aptitudes, cognitive skills or perceived “cultural” fit based on their performance.
- **Monitoring software** – rates employees based on their keystrokes.

XPO

Regulating AI

JacksonLewis

Regulating AI

Federal Developments

May 2023

- EEOC Issues Technical Assistance: Assessing Adverse Impact in Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures Under Title VII of the Civil Rights Act of 1964.

August 2023

- First EEOC consent decree with AI-related claims

- OFCCP revises their itemized listing to include AI system documentation

October 30, 2023

- President Biden signs Executive Order on Artificial Intelligence (rescinded in 2025 by President Trump)

April 29, 2024

- DOL and OFCCP releases new guidance on AI in employment practices.

January 23, 2025

- President Trump signs Executive Order on Artificial Intelligence titled “Removing Barriers to American Leadership in Artificial Intelligence.

April 23, 2025

- President Trump directs all agencies to deprioritize enforcement of statutes and regulations that include disparate impact liability.

Regulating AI (cont'd)

State Developments

January 2020

- Illinois' Artificial Intelligence Video Interview Act

July 2023

- New York City's Local Law 144

February 2026

- Colorado Artificial Intelligence Act

Illinois' Artificial Intelligence Video Interview Act (effect. 1/1/20)

1. **Notification and Consent**: Employers must notify applicants that AI will be used to analyze their video interviews, provide information on how the AI works, and obtain consent from the applicants before proceeding with the AI analysis.
2. **Data Handling**: The Act restricts the sharing of applicant videos to only those necessary for evaluating the applicant's fitness for a position. Additionally, upon request, employers must delete the video interviews and instruct others who received copies to do the same within 30 days.
3. **Demographic Reporting**: Employers relying solely on AI analysis for video interviews ***must collect and report demographic data, including the race and ethnicity of applicants, to ensure there is no racial bias*** in the hiring process.

New York City's Local Law 144 (effect. 1/1/23)

1. **Scope of Application**: The law specifically applies to employers and employment agencies within New York City that use AEDTs for employment decisions.
2. **Notice Requirement**: Employers must provide notice to candidates and employees about the use of AEDTs in the hiring or promotion process. This includes offering candidates an opt-out option.
3. **Bias Audit Requirement**: The law requires a bias audit to be conducted by an independent auditor within one year prior to the use of any AEDT. The results of this audit must be publicly available, and the audit ***must ascertain the selection rate for each race/ethnicity and sex category, as well as the impact ratio for each category***.

Colorado Artificial Intelligence Act (effect. 2/1/26)

1. **Notification, Consent and Rights**: Developers and Deployers must provide notice of the use of high-risk AI systems used to make consequential decisions, including employment or employment opportunity. Consumers have a right to correct and appeal.
2. **Duty of Care:** Developers and Deployers have duty of care to protect consumers from algorithmic discrimination, defined as "unlawful differential treatment or impact" based on race, ethnicity and sex.
3. **Impact Assessment:** Deployers ***must complete an impact assessment*** of high-risk AI systems.
    - AG to implement rules regarding content and requirements of impact assessment.
4. **Reporting:** Disclosure requirements to attorney general regarding known or reasonably foreseeable risk of algorithmic discrimination.

Use of AI Tools by Employees

JacksonLewis

Two Avenues of Inquiry

- Does the AI tool create data privacy and security risk?
  - Data minimization challenges
  - Collection of extraneous information
  - Increased data breach footprint
  - Vendor management issues (including model training)
- Does it create risk under the AI Laws?
  - Are employees using it to “substantially assist” with “consequential decisions”?
  - Are there ways to stay out of scope?
  - If not, are you ready to comply?
    - Impact assessments
    - Notices
    - Opt-outs

Starting Point Needs to be: What Tools are Your Employees Using and Why?

Popular tools and use cases:

- Chatbots (e.g., ChatGPT): Q&A re employment policies and benefits, drafting emails, summarizing documents, retrieving data, tracking receipt of information and sending reminders, planning and calendaring meetings, confirming data accuracy across systems or databases, thought partnership.
- Monitoring tools: Track employee productivity (online or physical (in case of wearables)) and compliance with Company policies.
- AI meeting assistants (aka AI notetakers): Record, transcribe, and generate notes from meetings.
- Video analysis software: To analyze video interviews, negotiations.

Have you vetted the tool and vendor?

Key vetting considerations:

- What tasks will the tool be asked to do (e.g., taking meeting notes, drafting emails, summarizing documents, sifting through resumes, monitoring employee productivity, etc.)?
  - Do those tasks align with the tools intended purpose(s)?
- What controls does the tool make available to prevent unauthorized data access, use, and disclosure, and algorithmic bias?
- What data will the tool process? Is that data from internal or external sources? Will it be used to train the models?
- Where will data processed by the tool be stored (e.g., on Company systems, on the vendor's systems, on another third-party's systems)?
- Does the vendor have data privacy and security certifications? Does it have robust policies and procedures? Has it had recent data breaches?

Do you have contractual protections?

Key contractual considerations:

- Training of models
- Processing limitation
- Access and disclosure limitations
- Audit rights
- DSAR assistance
- Security safeguards
- Retention
- Subcontracting

Fun with hypos!

JacksonLewis

Hypo #1: The AI notetaker conundrum

Bob hates taking notes during meetings because he feels like doing so detracts from his participation. Bob recognizes, though, that not having detailed meeting notes is interfering with his ability to do his job. He often walks away from meetings without a clear understanding of the action items he's responsible for and he regularly finds himself digging through emails to confirm the details of a group decision. . . only to realize the decision was made during a meeting for which he doesn't have good notes. Bob considers himself tech-savvy and, in a blog post about several cutting-edge AI tools coming to market, identifies the solution to his problem: An AI bot that can attend videoconferences, create a transcript of the discussion, and generate a list of key takeaways. Bob has a videoconference scheduled for the next morning and (excitedly) adds the bot to the meeting. What could go wrong?

Hypo #1: The AI notetaker conundrum [cont'd]

- Notice requirements (e.g., wiretap, invasion of privacy, CCPA).
- Bot will likely collect extraneous "off-the-record" statements during breaks in the meeting, creating privacy and employment risk.
  - "Sorry I was late joining, I was finishing up my therapy appointment"
  - "I can't make Thursday's meeting because of [religious holiday]"
  - "Dude, Bob was hammered at the happy hour yesterday"
- Bot may circulate that information more broadly than is reasonable or desirable, increasing legal risk and creating interpersonal conflict.
- Transcripts may be discoverable, driving up ESI costs and generating unwelcome surprises

Hypo #2: The HRIS "Help" Bot

Bob's an anxious guy and he's feeling overwhelmed. He's thinking about requesting a leave of absence or a work-from-home accommodation, and is also considering whether to seek treatment from a psychologist. Bob feels awkward discussing his situation with HR, so he instead logs onto the Company's HRIS platform, tells the "Help" bot about his troubles, and asks it two questions: (1) am I entitled to work from home or take a leave of absence, and (2) does my health insurance cover mental heath treatment? The Company expected employees to ask the "Help" bot less thorny questions like "How much PTO am I entitled to?", "What holidays do I get off?", and "How do I change my direct deposit?". It didn't occur to the Company that employees might it ask it questions like those Bob did. Any concerns?

Hypo #2: The HRIS "Help" Bot [cont'd]

- Bob is disclosing confidential medical information . . .
  - Where will that information be stored?
  - Who will have access to it?
  - Will it be used to train the model?
  - Do the bot developer's terms include appropriate data privacy and security provisions?
    - Do those terms prohibit inputs containing PII?
- Bob is discussing thorny accommodation and leave management issues . . .
  - What will the bot say in response?
  - Will the Company be deemed on notice of the need for interactive discussions?

Hypo #3: How much does Sally make?

Bob's bored. He opens the Company's internal chatbot, which is integrated with its suite of applications, including its document management system. Bob starts asking the bot random questions about his colleagues. The first few go nowhere, but, when Bob asks "How much does Sally Sanders in accounting make," the bot provides him a direct answer and links—as support for its response—to a spreadsheet saved in the Company's document management system that lists the prior year's compensation for every employee of the Company. Bob has never seen this spreadsheet, has no idea where on the document management system it's stored, and has no business need for this information. Why did the bot give Bob this response?

Hypo #3: How much does Sally make? [cont'd]

- Chatbots integrated with internal applications rely on user permissions established by the Company. If those permissions are overly permissive—meaning that users have access to more than they should—the bot may help employees surface sensitive information they would otherwise be very unlikely to find.
- If the Company hasn't undergone a recent data mapping exercise, it may not have a good handle on what's stored where—so even if its permissions are tight, there may be materials stored in folders Bob appropriately has access to, but that shouldn't be there (e.g., materials that are there because of the carelessness of other employees, or the Company's failure to archive and purge old data).

Hypo #4: I think we need to fire Rita

Bob receives a complaint from Jim. Jim reports that his manager, Rita, has repeatedly harassed him because of his religious beliefs and, to prove it, shows Bob a video of Rita repeatedly using religious slurs in the workplace. The video is disturbing and Bob recommends to his supervisor, Sonia, that the Company fire Rita. Should Sonia accept Bob's recommendation?

Hypo #4: I think we need to fire Rita [cont'd]

Not yet!

- AI-generated deep fakes are increasingly credible and easy to create. Even apparently "smoking gun" evidence needs to be viewed with caution.
- Verifying the authenticity of that evidence will become increasingly important.
- But be mindful to privacy issues: In collecting verification evidence from the complainant, the accused, and witnesses, collect only what's needed, limit access, and limit retention.
- You'll likely need to rely more heavily on technical experts – e.g., digital forensics firms specializing in video analysis, activity log analysis, etc.

Using AI to Drive Employment Decisions

JacksonLewis

Disparate Impact, Treatment and the Black Box

- One advantage of AI solutions is the efficiency by which data may be processed and employment decisions made
- What if the algorithm is considering a protected characteristic?
  - We must be concerned about disparate treatment. How will we know?
    - Even if the data variables being considered are sound, we must be careful to monitor for disparate impact
- Peering into the “black box”

Disparate Impact Analysis

Analysis	Rate for Women	Rate for Men	Hiring Rate of Women vs. Men	Standard Deviation	Shortfall
Women vs. Men	1/10 .10	20/100 .20	50%	0.77	0
Women vs. Men	10/100 .10	200/1000 .20	50%	**2.43**	**9**
Women vs. Men	100/1000 0.10	2000/10000 0.20	50%	**7.67**	**90**

To Validate or Not to Validate

- The 1978 Uniform Guidelines on Employee Selection Procedures or UGESP
  - "*These guidelines apply to tests and other selection procedures which are used as a basis for any employment decision*"

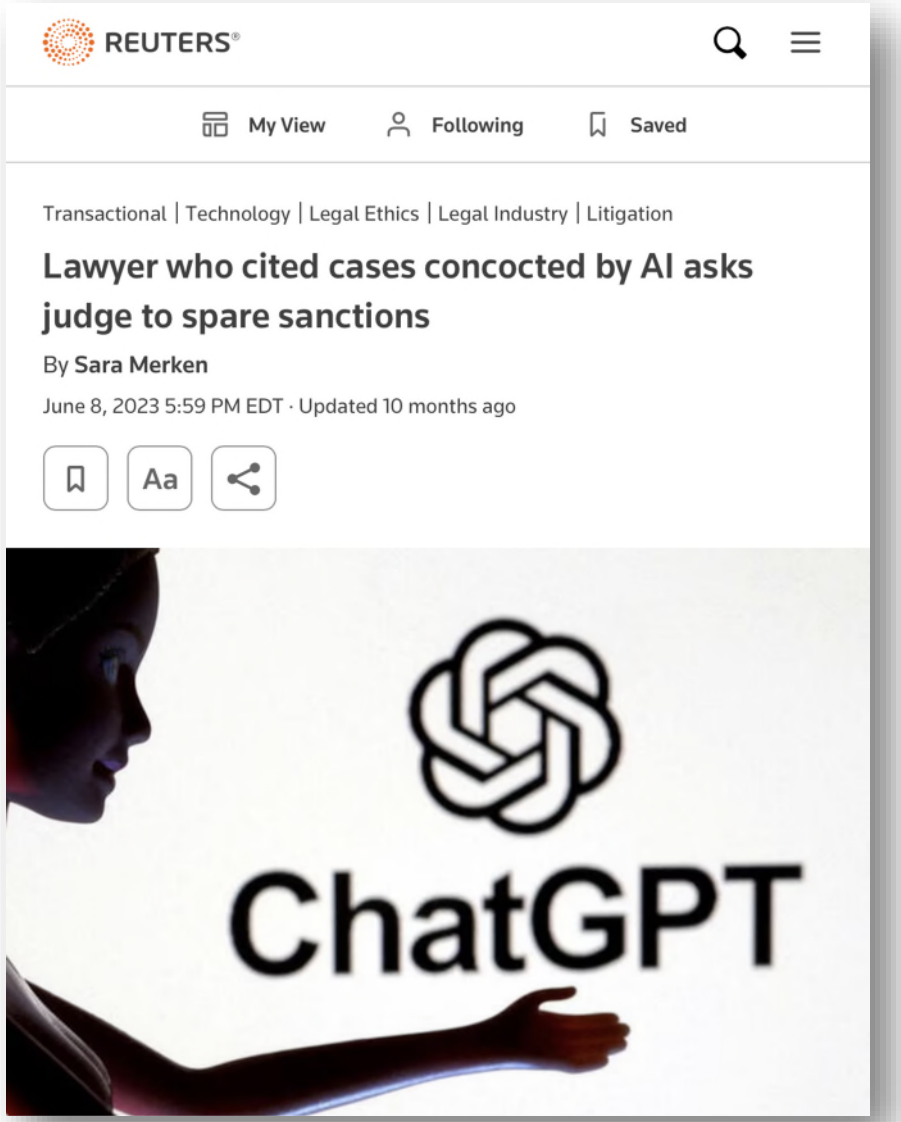
    "*The use of any selection procedure which has an adverse impact on the hiring, promotion, or other employment or membership opportunities of members of any race, sex, or ethnic group will be considered to be discriminatory and inconsistent with these guidelines, unless the procedure has been validated . . .*" (emphasis added)

Should Data Alone or Algorithmic Results Drive Every Decision?

Algorithms could be tainted by bias — intentional or not

- Without safeguards, overreliance on algorithms to drive decisions could raise a host of issues
- Similarly, overreliance on generative AI outcomes could lead to consequences (e.g., hallucinations, inaccurate results, flawed outcomes)

It’s a question of balance!



Mitigation

JacksonLewis

Mitigation Measures

- Take the time to learn about the tools your employees want to use and how they want to use them; decide which tools and use cases to permit, and safeguards to implement; and develop process to vet additional tools.
- Decide what data employees should be permitted to use to prompt tools.
- Assess whether you can remain outside the scope of the AI Laws; if you can’t, prepare to comply.
- Be transparent with employees, customers, and clients about the use of AI by your employees.
- Manage your vendor risk.
- Be mindful of data minimization and retention—more and longer is often not better.

Questions?

JacksonLewis

Don’t Miss a Beat!

Scan the QR code for updates and insights from Jackson Lewis attorneys, delivered straight to your inbox.

Thank you.

JacksonLewis