Association of Corporate Counsel
CHICAGO

AI in the Workplace – *Regulatory Updates and Mitigation of Risk*

JacksonLewis

Presenter

Eric Felsberg

Principal, Long Island

631-247-4640

Eric.Felsberg@jacksonlewis.com

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

What's on the Mind of Regulators?

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.”
- The importance of transparency.

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**

The Developing AI Legal Landscape

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- President Biden signs Executive Order on Artificial Intelligence (*rescinded* in 2025 by President Trump).

Regulating AI

Federal Developments (cont'd)

April 29, 2024

- DOL and OFCCP release 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

State Developments

January 2020

- Illinois' Artificial Intelligence Video Interview Act

January 2023

- **New Jersey** proposes Assembly Bill 4909 requiring companies to notify candidates of the use of AI when screening applicants
- **California** proposes AB 331 and SB 721 (Becker) modifying use of AI in automated-decision systems
- **Vermont** proposes Assembly Bill 114 restricting the use of AI in employment decision making

February 2023

- **Massachusetts** introduces House Bill 1873 restricting the use of AI when making employment-related decisions
- **Washington, D.C.** introduces *"Stop Discrimination by Algorithms Act of 2023"*

Regulating AI

State Developments (cont'd)

July 2023

- New York City's Local Law 144

October 2025

- Revisions to Title 2 of the California Code of Regulations will govern the use of AI-based tools in California starting October 1, 2025

January 1, 2026

- Texas Responsible AI Governance Act (TRAIGA)
- Illinois AI in Employment law (HB 3773)

February 2026

- Colorado Artificial Intelligence Act

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.***

California's AI Regulations (effect. 10/1/25)

1. **Scope of Application:** The new regulations apply to all employers in California and pertain to any automated decision system (ADS) — not just advanced "AI" tools, but also those using selection criteria for hiring, promotions or training.
2. **Notice Requirement:** Employers must preserve ADS-related records, including dataset descriptors, scoring outputs, and audit findings, for four years.
3. **Bias Audit *Recommended*:** The regulations emphasize the value of bias audits or other efforts to avoid unlawful discrimination. In discrimination cases, courts and agencies may consider the quality, scope, recency, results, and employer response to bias testing. The absence of such evidence may weigh against employers that choose not to evaluate their ADS.
    - Employers are prohibited from using ADS or criteria that result in discrimination based on protected categories under FEHA and must accommodate religious and disability needs.

Texas Responsible AI Governance Act (TRAIGA) (effect. 1/1/26)

1. **Scope of Application:** The new regulations apply to any individual or entity, including government agencies, developing AI systems in Texas, offering a product or service used by Texas residents, or promoting, advertising, or conducting business in the state.
2. **Unlawful Discrimination:** TRAIGA prohibits a person from developing or deploying an AI system with the intent to unlawfully discriminate against a protected class in violation of state or federal law.
   - Disparate impact alone is not sufficient to demonstrate an intent to discriminate.
3. **Disclosure to Consumers:** TRAIGA requires governmental agencies and healthcare services that make AI systems available for consumers to disclose when consumers are interacting with the AI system either before or at the time of the interaction.

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.

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."*

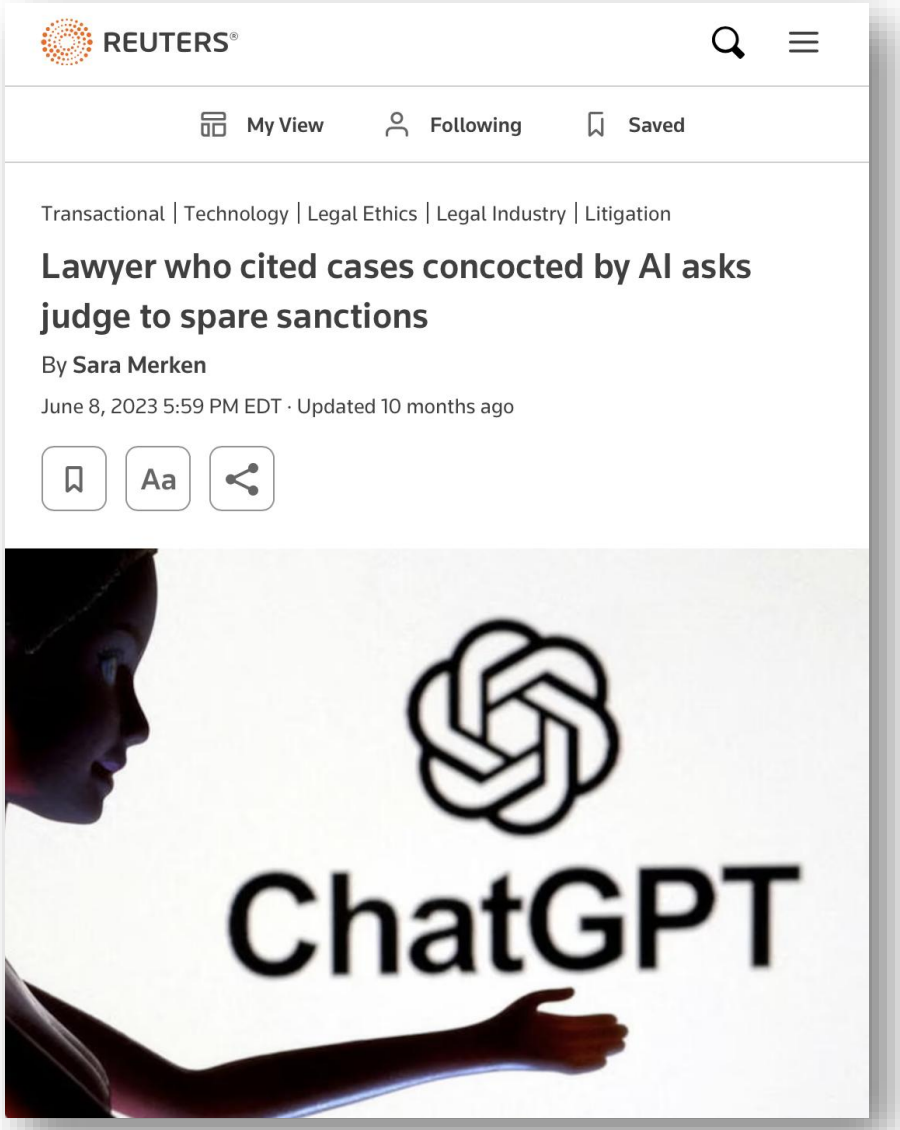
  "The use of any selection procedure which has an adverse impact on the hiring, promotion, or other employment or membership opportunities of members of any race, sex, or ethnic group will be considered to be discriminatory and inconsistent with these guidelines, unless the procedure has been validated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

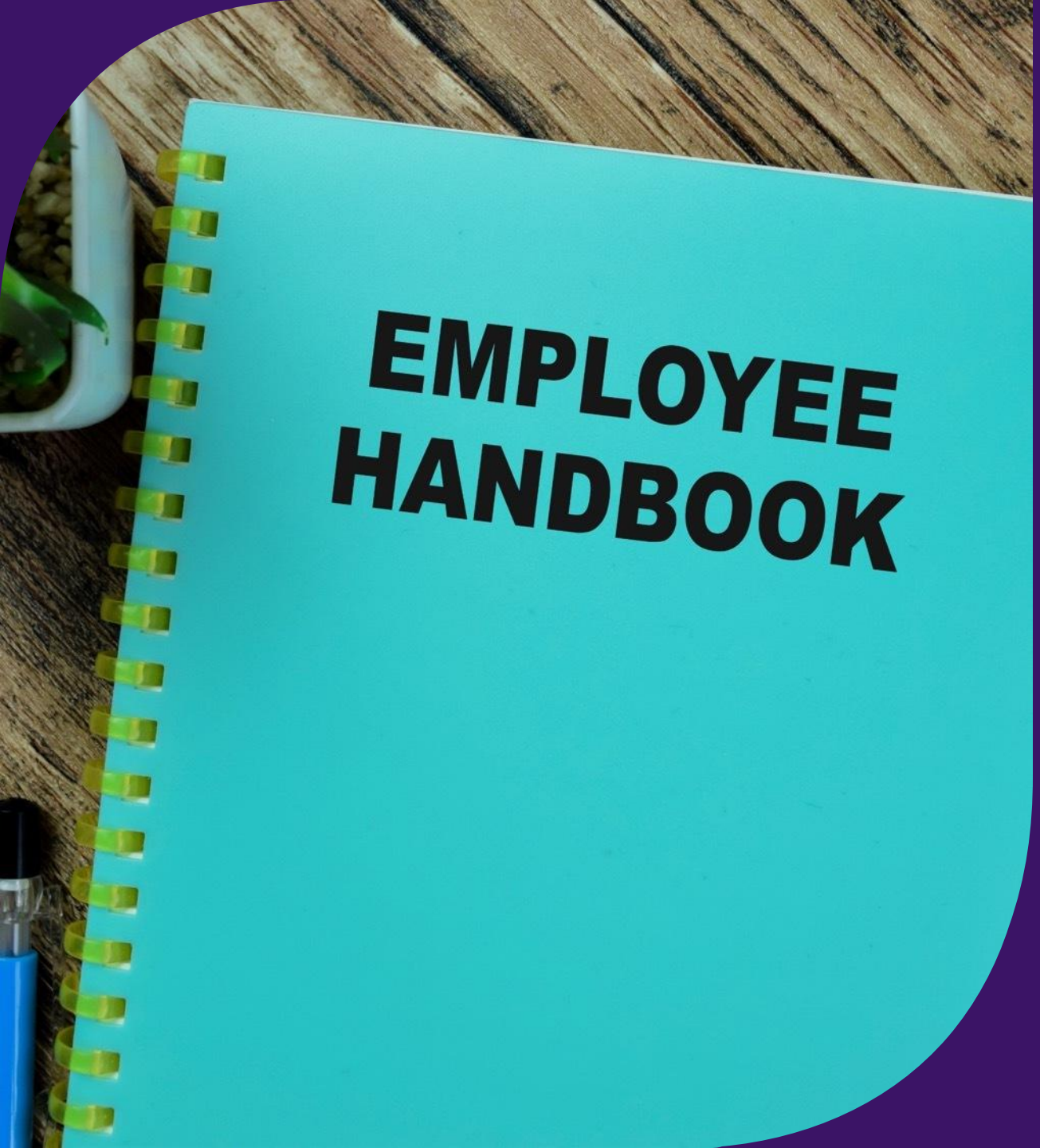


Mitigation

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.



Governance: Establishing Organizational Policies

Governance: Establishing Organizational Policies

- Establish a governance structure
- Form a multidisciplinary governance committee
- Develop AI policies to address issues such as:
  - Confidentiality, Data Privacy, and Data Security
  - Use of Approved AI Tools and Monitoring
  - AI Training
  - Intellectual Property
  - Bias

Appendix - Case Studies

JacksonLewis

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?

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

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?

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?

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?

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).

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?

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.

Thank you!

JacksonLewis