

Managing New Risks and Opportunities from AI in the Workplace

April 25, 2025

Bob Quackenboss, Partner, Labor & Employment
Reilly Moore, Associate, Labor & Employment

Presenters



Robert Quackenboss,
Partner
Labor and Employment
Washington, DC
New York, NY



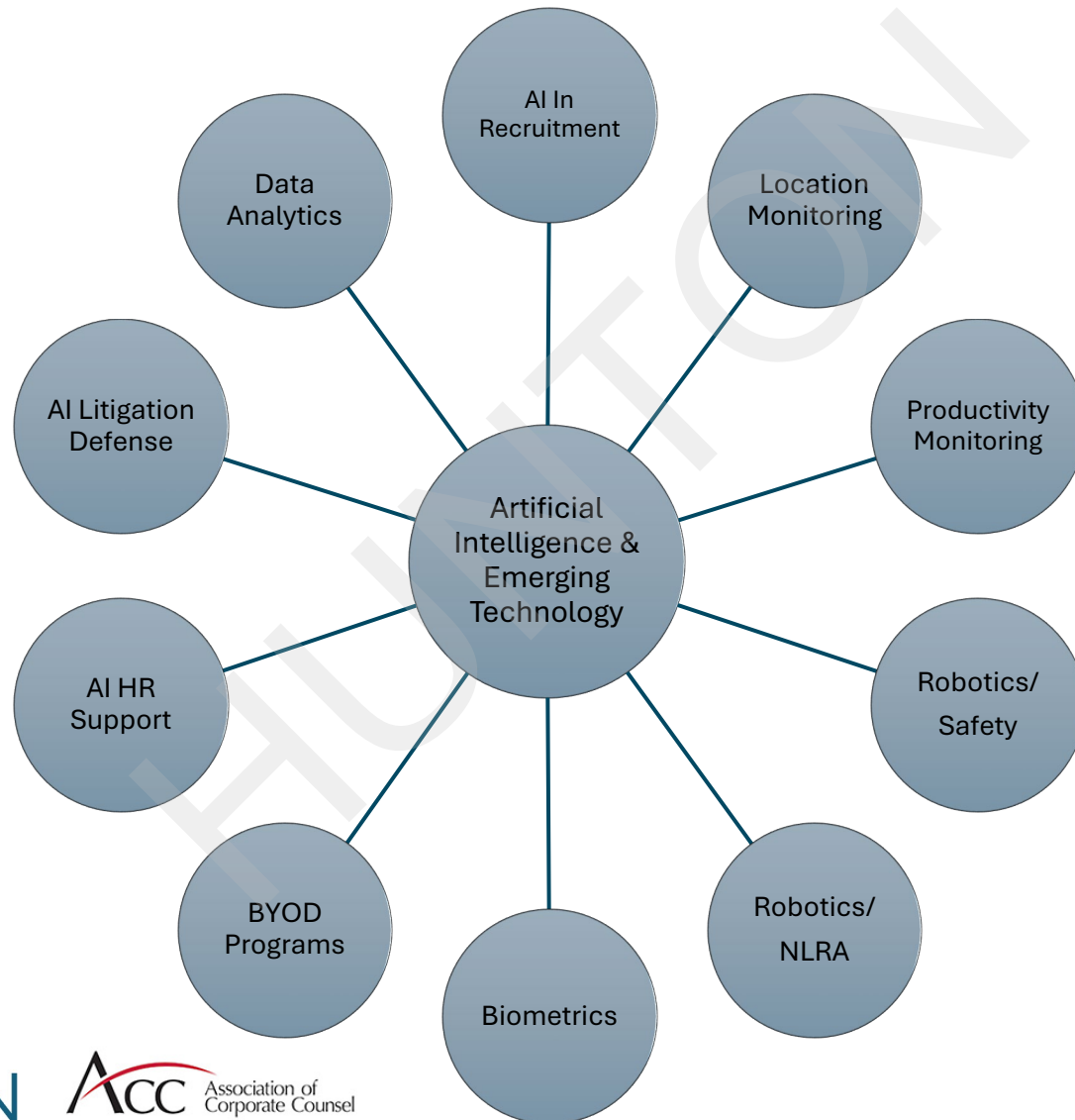
Reilly Moore
Associate
Labor and Employment
Richmond, VA



Aisha Jorge Massengill
Former Head of Employment Law at
Sonos and Under Armour
Columbia, MD

© 2025 Hunton Andrews Kurth LLP. Attorney advertising materials. These materials have been prepared for informational purposes only and are not legal advice. This information is not intended to create an attorney-client or similar relationship. Please do not send us confidential information. Past successes cannot be an assurance of future success. Whether you need legal services and which lawyer you select are important decisions that should not be based solely upon these materials.

Labor and Employment Emerging Tech Group



Relevance of AI – Why Does AI Matter?

- Increased prevalence – if your company isn't using AI yet, chances are that it will soon
 - McKinsey Study: 78% of companies use AI as of 2024 (up from 20% in 2017)
- Automated decision-making tools require proactive monitoring
 - Decisions may not cross your desk before they occur – need to understand how to issue-spot for AI risks
- Emphasis on merit-based hiring, attacks on DEI
 - AI programmed based on historic legal guidance may no longer make sense
- Increasing regulation
 - States, localities taking more active role in AI regulation, deals with vendors and/or designers should account for potential change

"Lawyers may not be replaced by AI, but lawyers who don't understand AI may be replaced."

Agenda

- What is Artificial Intelligence and Generative AI? (5 min. - Bob)
- Popular AI Tools for the Workplace (10 min. - Bob)
- The Developing Law Regulating AI in the Workplace (20 min. – Reilly)
 - Federal and State Overview
 - Bias and Discrimination
 - Privacy Issues in Workplace AI (include social media AI)
 - Copyright / IP issues
- Best Practices and Compliance (25 min.) (Bob / Reilly)

Artificial Intelligence and Generative AI

- **Artificial Intelligence**
 - process involving designing machines meant for carrying out work only done by brains before.
 - “Machine-based systems that...make predictions, recommendations or decisions influencing real or virtual environments.”
 - Intelligent Resume Screening
 - Automated Candidate Sourcing
 - Testing Software
 - Performance Management Software
- **Generative Artificial Intelligence – goal of GAI is human-level intelligence**
 - ChatGBT, Siri, Alexa, Copilot, content generation, art creation, language translation

Popular Workplace AI Tools

- **Chatbots**
- **Automated Candidate Sourcing**
- **Intelligent Resume Screening**
- **Testing Software**
 - Measure cognitive skill.
 - Analyze compatibility.
- **Performance Management / Retention**
 - Data-driven performance analysis.
 - Productivity Monitoring
 - Predict future behavior.
- **Generative AI (ChatGPT)**

What is AI in Employment Screening?

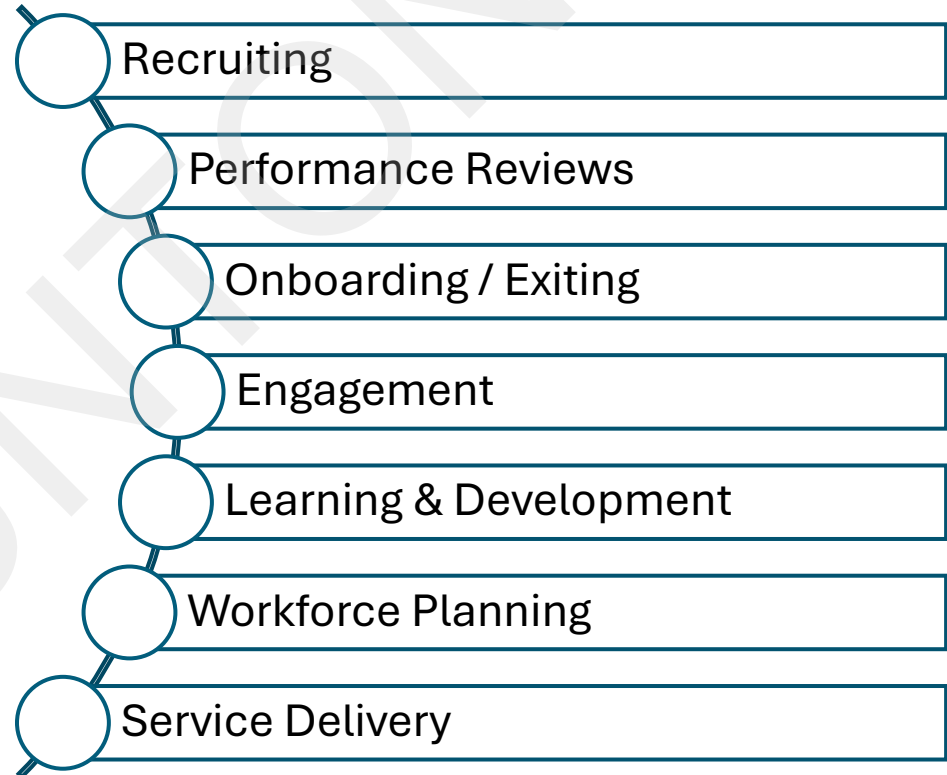
Artificial Intelligence uses computing to perform tasks which typically require human intelligence. Typical tasks include:

- Understanding natural language
- Learning
- Reasoning
- Problem solving

This technology impacts critical human capital business processes such as recruitment and talent management, driving automation and facilitating decision making.

Why use AI in employment screening?

- Gain insights into the talent pool
- Automate high-volume tasks
- Increase consistency and quality of decisions
- Decrease time to hire
- Decrease turnover
- Optimize ROI on individual employees and teams



Productivity Monitoring: Examples of Available AI

Keystroke Monitoring

- Tracks and records keyboard activity, whether into web browsers, instant messages, e-mails, applications, documents or other programs.

Activity Tracker

- Monitors/tracks web browsing, records which applications are used and the amount of time spent on each. May take periodic screenshots.

Email Tracking

- Measures how many emails employees are sending and receiving, how much time spent on messages, and identifies busiest days and times.

Data Loss Prevention Solution

- Detects anomalous patterns or behavior through keystroke logging, network traffic monitoring, and natural language processing.

Facial Recognition Tool

- Uses workers' webcams for various purposes, including to record when an employee had stepped away from his computer.

Engagement Algorithm

- Used to detect employee emotions, unhappiness, and disengagement. Looks for patterns to predict when workers are likely to quit or engage in behavior adverse to the company.

Productivity Monitoring: Benefits To Your Workplace

Learning how employees work best

- **Identify** tools employees need, discover employees' most productive periods and which teams work best.

Decreasing distractions

- **Identify** websites and activities that create distraction. Reduce, block or prohibit use.

Keeping employees on task

- Monitored employees tend to stay on task more; The Hawthorne Effect.

Keeping employees accountable

- If employee did not finish a project, you may be able to see why.

Rewarding exceptional performance

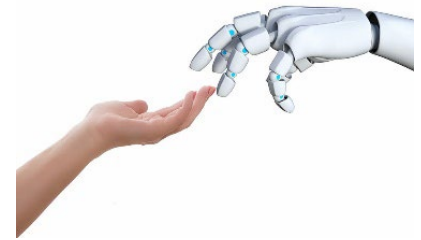
- **Identify** and reward productivity.

Balancing workloads

- **Identify** those that are overworked and those that do not have enough to do. Redistribute workloads appropriately.

Starting a conversation

- May help managers identify earlier those employees who are struggling and start a conversation to help the employee improve.



AI Retention Tools



AI designs **on-boarding** tailored to new employee's experience, skills, interests and cultural fit.



Predictive analytics to identify employees at risk of leaving and propose intervention strategies.



AI tailors **training** and skill development.



AI **succession planning** and talent pipeline.



Specialized **employee satisfaction surveys**, with pattern detection.



Integrates **DEI considerations** with all of the above.

Generative AI: Impact on Hiring and the Workplace

○ As a Tool for Applicants

- Is an application, essay or writing sample truly representative of the applicant's skills?
- Specialized descriptors and turns of phrase in resumes.
- Correspondence before and after interviews.
- Interview preparation: cheat sheets on appropriate responses and jargon.
- **RISK**: GAI misrepresents the applicant's skills and experience.
- **MITIGATION**: Specific acknowledgments and representations about sourcing.

○ As a Tool for Employees / Management

- Internal work product – analysis, recommendations, performance assessments.
- External / customer facing content.
- **RISK**: Inaccurate / incomplete data as GAI source material.
- **RISK**: Loss of customer confidence / lawsuits.
- **RISK**: Discrimination under Title VII and EEO statutes.



Legal Guardrails for the Use of AI / GAI in Workplaces

Recap AI: Disparate Treatment v. Disparate Impact

- **Recap: Examples of Common Uses in the Workplace**
 - Recruiting; resume screening; interview analysis; productivity monitoring; performance evaluation.
- **Disparate Treatment**
 - Requires proof of intent to discriminate.
 - Intent can be proven through direct or circumstantial evidence.
 - Less likely AI would be used to intentionally discriminate.
- **Disparate Impact**
 - Does not require proof of intent.
 - Focuses on effect of facially neutral policy or practice.
 - Often involves statistical expert analysis.
 - Most likely form of discrimination through use of AI.



NLRB Guidance

- **Electronic Monitoring and Algorithmic Management of Employees Interfering with Exercise of Section 7 Rights**
 - Issued October 31, 2022, but Rescinded in February 2025
 - Critical of electronic monitoring and algorithmic management of employees
 - Former GC Abruzzo: “I will urge the [NLRB] to find that an employer has presumptively violated the [NLRA] where the employer’s surveillance and management practices, viewed as a whole, would tend to interfere with or prevent a reasonable employee from engaging in activity protected by the [NLRA].”
 - Acting GC Cowen rescinded Abruzzo surveillance memo, along with many others. To date, unclear how new GC will handle AI tools, but can expect more deference to employer priorities, even if technology has some potential to interfere with or restrict protected activity.
 - Still could be problematic if it results in actual interference with protected activity, or active, out-of-the-ordinary surveillance of employees.
- **Courts Skeptical of NLRA’s Reach into Routine Surveillance Issues**
 - *Stern Produce v. NLRB*, 97 F.4th 1 (D.C. Cir. 2024), overruling Board decision.
 - Supervisor’s reminder to truck driver not to cover in-cab camera did not violate NLRA.
 - Court: Board decision showed “just how far [NLRB] strayed from its statutory mandate.”

Employment Discrimination Issues and EEOC

- **EEOC Rescinded Formal AI Guidance issued under Biden Administration**
 - Trump executive order instructed government-wide review of guidance that restricted use of AI
- **But Title VII, ADA and Related Laws Still Apply**
 - EEOC guidance lacks force of law, decision to rescind guidance does not impact private plaintiffs' ability to pursue claims
 - Prohibitions on discrimination, failure to accommodate, retaliation
 - Tracking or wearable technology could create ADA issues
- **AI Programs that Include Diversity Metrics May be Questioned**
 - EEOC Guidance document on "DEI-Related Discrimination at Work" targets quotas or programs that make *any* decisions based on protected characteristics
 - Includes "diverse slate" programs that consider pre-employment information about race, disability, etc., in any way
 - Potential Problem: AI programmed to encourage or suggest a diverse applicant pool, even if AI not used for the final hiring or promotional decisions

Executive Orders and Actions

- **Removing Barriers to American Leadership in Artificial Intelligence**
 - Issued January 23, 2025
 - Revoked Biden EO that addressed standards for safety and security, privacy, equity and civil rights, worker protections, etc.
 - Goal of Trump EO: “develop AI system that are free from ideological bias or engineered social agendas.”
 - Orders development of “Artificial Intelligence Action Plan” within 180 days or order (July 22, 2025)
 - Align Biden OMB memos on AI governance measures to meet Trump policy objectives
- **Federal Policy in Flux**
 - EEOC, OFCCP removed prior guidance on AI in employment from respective websites
 - DOL aligning behind lesser regulatory approach, but “Action Plan” may dictate federal approach moving forward

States Taking Action on AI: Colorado

- **Colorado Artificial Intelligence Act**
 - First comprehensive state law governing AI hiring tools.
 - Effective date: February 1, 2026
 - Regulates “high-risk artificial intelligence systems”
 - Systems that make, or serve as substantial factor in making, “consequential decisions,” including decisions related to employment
 - Imposes obligations on both developers and users of AI technology
 - Users (like employers) must disclose intent to use the tools to applicants, employees or other consumers in advance
 - Must provide explanations for adverse decisions made by AI
 - No private right of action – enforcement by CO Attorney General
- Similar to federal Fair Credit Reporting Act – focused on advanced disclosure, notice of adverse action and imposes

States Taking Action on AI: California

○ **A.B. 1018 (Proposed)**

- Similar to Colorado law regulating high-risk AI
- Broad definition of “employment-related decision”
 - Anything that affects wages, benefits, other compensation, hours, work schedule, performance evaluation, hiring, discipline, promotion, termination, job tasks and responsibilities, assignment of work, access to work and training opportunities, productivity requirements, workplace health and safety, or other terms or conditions of employment
- Includes steeper penalties and potential for private right of action
 - Private Attorneys General Act
 - Civil penalties up to \$25,000 per violation

○ **Attorney General’s Legal Advisory on Existing Law**

- Formal guidance on how AI fits in existing legislative framework
- Civil rights (and other state laws) apply equally to use of AI
- California Consumer Privacy Act (CCPA) implicated

States Taking Action on AI: Illinois

- **Artificial Intelligence Video Interview Act**
 - Employer conducting AI-based video interview **must** provide applicant advance notice that AI may be used, inform applicant how AI works, obtain applicant's consent to evaluation by AI, and delete video within 30 days of applicant's request.
 - Employer **cannot** share applicant video **except** with people whose expertise is necessary to evaluate applicant.
 - Employer relying solely on AI analysis to select applicant for in-person interview **must** annually collect and report information to Illinois Department of Commerce and Economic Opportunity:
 - ethnicity and race of applicants not selected for in-person interviews;
 - ethnicity and race of applicants hired.
- Illinois Department of Commerce and Economic Opportunity **must** analyze data and report by July 1 of each year whether data discloses racial bias.

States Taking Action on AI: Maryland

○ **Regulates facial recognition services technologies during job interviews**

- Employers are **prohibited** from using facial recognition services to create facial template during applicant's interview absent signed waiver by applicant.
- Signed waiver must contain applicant's name, interview date, applicant's consent to use of facial recognition during interview, and acknowledgment that applicant read waiver.

New York City Regulation of AI Decisional Tools

- **Regulates Automated Employment Decision Tools (AEDTs)**
 - Employer only can use AEDT to screen candidate for employment **if** such tool has been subject of bias audit conducted **no more than one year prior** to use of tool and summary of audit and tool's distribution date has been made publicly available on employer's website.
 - Employer using AEDT to screen candidate **must** notify candidate at least 10 business days before using tool that it will use tool to assess candidate, job characteristics and qualifications tool will use in assessing candidate, and candidate can request alternative selection process or accommodation.
 - Employer shall make information about type of data collected for AEDT, source of such data, and employer's data retention policy available within 30 days of written request by candidate unless such information is disclosed on employer's website, or such disclosure would violate law or interfere with law enforcement investigation.

Other State Level Actions

- **State legislation facing difficult paths to becoming law**
 - **Virginia** – Governor vetoed comprehensive AI legislation
 - **Connecticut** – Governor vocally opposed to comprehensive AI legislation proposed by state assembly
 - **Texas** – Proposed bill lacks momentum toward passage
 - Similar bills proposed, but unlikely to succeed in Georgia, Hawaii, Maryland, New Mexico and Vermont
- **AGs in some states releasing compliance guidance**
 - **New Jersey AG** (January 2025)
 - Summarizes research on AI tools, and finds legality will depend on the circumstances and the nature of the specific programming
 - **Oregon** (December 2024)
 - Addresses AI in the context of state privacy, unfair trade and Equality Act
 - **Massachusetts** (April 2024)

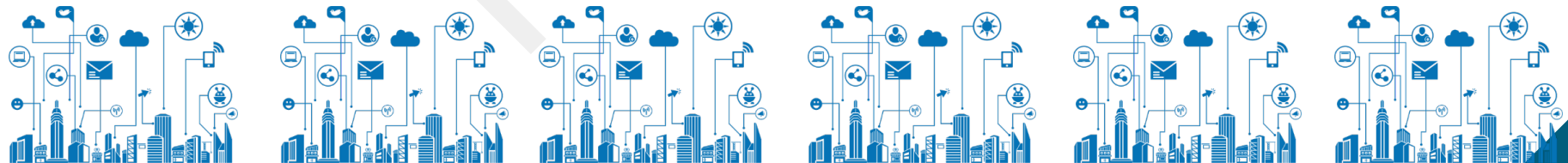
AI and Candidate Selection: How Algorithms May Discriminate

○ **AI can reinforce institutional homogeneity**

- Most algorithms need training data (e.g., resumes of high performing employees).
- Results will mimic training inputs.
- If training models are homogenous, results may also reflect lack of diversity.
- Or, vice versa, if models mandates diverse candidate, AI may continue, even if employer policy has changed

○ **AI may consider biased variables**

- Algorithms may develop preferences for neutral criteria that are proxies for unintentional discrimination.
 - E.g., Algorithm may favor zip codes close to the office which can serve as a proxy for race discrimination.
 - E.g., Algorithm may favor ".edu" e-mail addresses, prejudicing older workers (ADEA concern).



Adverse Impact in Artificial Intelligence Tools



What if you train your AI tool on incomplete or irrelevant data?



What if your AI model is missing vital context regarding goals?

Assessing AI Compliance with Discrimination Law

- Does AI programming explicitly factor in any protected characteristics?
- Does AI rely on historical data that implicitly factors in diversity goals or statistics?
- Does programming consider accuracy of applicant or employee inputs (i.e., spelling, grammar, etc.) that may adversely impact non-native speakers?
- Does AI make or substantially impact any final employment decisions?
- Does analysis of AI outputs indicate different outcomes than human-driven process? More diverse? Less diverse? Any statistical difference regarding a protected trait?
- Does any tracking or assessment program accounts for disabilities or accommodations that employees or applicants may receive?
- Are the data points considered by the AI tools defensible as job-related and consistent with business needs?
 - May vary by job position

Privacy Considerations

- Data is the fuel that powers AI technology
 - Need to large volumes of data to make AI tools effective operates in tension with privacy requirements that protect consumer data from misuse or improper disclosure
- At least 19 U.S. states have comprehensive and broadly applicable privacy laws protecting consumer data
- Many AI tools are “black box” – data goes in, but then can’t find it
 - Data becomes inextricably intertwined with the AI program itself
- Business-to-business confidentiality obligations
 - Contractual relationships may impose privacy or use obligations that AI tools jeopardize

Applying Confidentiality / Data Protection Principles to AI

Need to consider the challenges and tradeoffs with processing personal information for AI in accordance with data protection principles:

- **Lawfulness**
 - Will the legal basis for running the AI analysis or report require consent?
- **Fairness**
 - Are there discriminatory or ethical implications?
 - Need to consider automated decision-making rights and restrictions.
- **Transparency**
 - Will maintaining a public privacy notice suffice?
- **Purpose Limitation**
 - Will you be gathering data for undetermined or secondary purposes?
 - Data hoarding is problematic.
- **Accuracy**
 - Is there a duty to correct or delete the raw data sets? Results?
- **Storage Limitation**
 - Are there bans on unlimited retention of data sets?
- **Security and Confidentiality**

Confidentiality / Data Protection

Challenges and Tensions

Data Protection Requirements	Tensions To Resolve	Artificial Intelligence
Collection limitation / Data minimization		Needs sufficient volumes of data for research, analysis, operation, training and to avoid bias
Purpose specification & use limitation		Uses data for new and unforeseen purposes beyond original scope
Legal basis for processing		Insufficient/limited variety of legal bases may undermine full range of AI applications
Retention limitation		Needs to retain data for AI training, deployment and oversight
Transparency		Operates in a black box and may produce unexplainable and unanticipated outcomes
Individual rights		Cannot always facilitate access, correction or explanation of the logic involved
Rules/restrictions on ADM		Based on ADM & no human involvement

Read more in CIPL's First AI Report on **Artificial Intelligence and Data Protection in Tension**

<https://bit.ly/2QUP2xy>

Productivity Monitoring: State Law - Regulations and Tort Claims

Some states have imposed greater limitations than federal law

- **Connecticut** and **Delaware** require employers to inform workers of email monitoring.
- **Colorado** and **Tennessee** require email monitoring policies.
- **California, Florida, Louisiana** and **South Carolina** guarantee citizens a right to privacy.
- **California** and **Illinois** require employers to obtain consent from third parties before intercepting emails sent to employees.
- **California, New York**, and **Massachusetts** have enacted spyware laws prohibiting access to personal devices without prior authorization.

Common Law Invasion of Privacy Claims

- Elements differ by jurisdiction
- Courts generally weigh the employee's reasonable expectation of privacy against the employer's legitimate business interest.



Productivity Monitoring: Legal Considerations

Electronic Communications Privacy Act (ECPA)

National Labor Relations Act (NLRB)

- Surveillance of employees engaged in concerted activity may be unfair labor practice.

The 4th Amendment

- May cover certain public employees. Prohibition against unlawful search and seizure.

General Data Protection Regulation

- Applies in the European Union. Requires necessity, awareness, and agreement.

California Consumer Protection Act (CCPA)

- Requires “notice at collection” at or before personal information collected.
- Identifies “browsing history, search history, and information regarding a [worker’s] interaction with an internet website, application, or advertisement” within scope.

State Social Media Password Protection Laws

- **Over 25 states** have laws that prohibit employers from requesting or requiring employees to provide credentials to their online personal accounts.

Best Practices and Compliance

Thinking About AI Correctly

- AI requires accurate and complete data and a thorough understanding of the project.
- Consult outside counsel and have frequent conversations with vendors.
- **Introspective Questions:**
 - How do I know AI is working?
 - How much AI? Which type of AI?
 - All HR processes? Some?
 - Which vendor to choose? What terms should vendor contract include?
- **Do not** blindly follow AI.

Threshold Questions: Is Your Workplace Ready ?

- Are all stakeholders informed and “on board?” Executives, managers, Human Resources, Legal, Unions, Administration / IT?
- Does Company culture welcome new technology? Is there a plan to bridge the skills gap?
- Does the vendor / designer provide effective written training materials and robust support for onboarding and troubleshooting?
- What is the goal of integrating AI? Cost savings? Efficiency? Headcount reduction?
- Will Company culture survive a RIF? Would it thrive from a RIF?
- Does HR have the resources, staff and support to administer and implement these vast changes?

Key Accountability Tools for AI

Leadership and Oversight

- DPO and senior management (boards, committees)
- Network of AI leads, lead legal counsel and privacy engineers

Privacy Reviews

- Risk and benefits assessment / document tradeoffs
- Identify measures to mitigate impact on individuals

Inventorying

- Document types of data and if/how they can be linked back to an individual
- Note how the data processing evolves and if the purpose of the processing changes

Policies and Procedures

- Incident Response Plans, Data Subject Rights Policy, Audit and Monitoring Procedures, Vendor Due Diligence, *etc.* to cover both the training and deployment phases of AI

Training and Awareness

- Involve privacy professionals and engineers
- Fairness and ethics training

Internal Supervision and Verification

- Complaints handling, redress mechanisms and remediation
- Ongoing monitoring, verification and mitigation

Recommended ML-Specific Privacy Terms

Consider requiring Machine Learning vendor to:

- Ensure fairness and prevent unwanted bias.
- Agree on regular updates and reviews of accuracy.
- Guard against changing population and concept drift.
- Use privacy enhancing technologies .
- Require appropriate safeguards and breach notification.
- Employ ethics-by-design.
- Ensure appropriate leadership and supervision of the ML process.
- Perform ongoing monitoring, audits, evaluation and training.
- Perform ML risk assessments.
- Implement risk-mitigating measures (e.g., embed human review of data output, maintain documentation).

AI Vendor Diligence Questionnaires – Key Questions

How does vendor balance accuracy with data minimization?

Has vendor conducted ML Risk Assessment and what was the outcome?

Is model's output determinative or used only as a recommendation?

Does ML model design allow identification and extraction of relevant data to respond to DSRs?

Has vendor incorporated human review?

How does vendor's accountability program include ML model?

Does vendor engage in data scraping practices to obtain data?

Does vendor keep data of customers separate?

How does vendor ensure fairness and accuracy, and prevent unwanted bias/potential discrimination?

Does vendor derive value from customer data analysis and re-use data for benefit of other customers?

In-House Best Practices Recommendations

- Provide clear written notice to applicants about the use of AI in your processes
- Consider providing an opt-out for objecting candidates and be clear about the availability of reasonable accommodations throughout the hiring process
- Require that use of AI tools on company systems go through a vetting process that documents the intended use and identifies ways that sensitive company information will be protected.
- At the point of tool adoption, establish clear procedures for human oversight. This may potential include convening a standing committee of cross functional partners: (HR, IT and Legal for example) to review re
- Make sure that any tool has been properly validated and is job related and consistent with business necessity
- Conduct annual impact assessments (preferably under privilege) to determine potential adverse impact

In-House Best Practices Recommendations

For existing employees, business should have:

- Written policies governing AI use
- Training programs for HR staff
- Clear procedures for AI system oversight
- Regular compliance reviews
- Documentation protocols

Questions?

Presenters



**Robert Quackenboss,
Partner**

rquackenboss@HuntonAK.com

(202) 955-1950



**Reilly Moore
Associate**

rmoore@hunton.com

(804) 788-8409



Aisha Jorge Massengill

Former Head of Employment Law at
Sonos and Under Armour

Ajorge23@yahoo.com

© 2025 Hunton Andrews Kurth LLP. Attorney advertising materials. These materials have been prepared for informational purposes only and are not legal advice. This information is not intended to create an attorney-client or similar relationship. Please do not send us confidential information. Past successes cannot be an assurance of future success. Whether you need legal services and which lawyer you select are important decisions that should not be based solely upon these materials.

Additional Resources

Hunton Employment & Labor Perspectives Blog:

Analysis and Development in Employment & Labor Issues

<https://www.hunton.com/hunton-employment-labor-perspectives/>

HuntonAK Insights

<https://www.hunton.com/insights/informed>



© 2025 Hunton Andrews Kurth LLP. Attorney advertising materials. These materials have been prepared for informational purposes only and are not legal advice. This information is not intended to create an attorney-client or similar relationship. Please do not send us confidential information. Past successes cannot be an assurance of future success. Whether you need legal services and which lawyer you select are important decisions that should not be based solely upon these materials.

Thank you!
