



# Navigating With Technology

Conor Neusel  
Zoe Spector

Thompson Coburn's Annual Labor,  
Employment and Employee Benefits Law Seminar

# Agenda



This presentation will delve into some of the ways that employers navigate with technology, including:

- Using **artificial intelligence** in recruiting, evaluating performance, and making termination decisions;
- How various state **biometric information privacy laws** can impact an employer's exposure to litigation; and
- Relying on **GPS tracking devices** to monitor employees' whereabouts and mileage when employees are required to drive for work purposes.

# Artificial Intelligence



- Benefits for Employers:
  - Efficiency in recruiting, screening resumes, rating job candidates
  - Removes human element of performance evaluations to help focus on deliverables and productivity measurements
  - Assistance in tracking employee performance and objective, results-driven termination decisions

# Artificial Intelligence



- Areas of Exposure for Employers:
  - Potential for unforeseen discriminatory impact
  - Risk of removing human element when reviewing employee performance and decisions to terminate
  - Privacy implications

# Artificial Intelligence in Recruitment



- Predictive analytics can save employers time and money during the recruiting, screening, interview, and rating stage
- When designed and implemented correctly, Artificial Intelligence tools can also help take out human biases and enhance diversity and inclusion in the workplace

# Artificial Intelligence in Recruitment



- If the Artificial Intelligence is poorly designed and not effectively deployed, it could lead to severe disparate impact toward applicants – even when the employer has the best intention in using the Artificial Intelligence

# Federal Law



- It is not a defense to a Title VII discrimination claim that the decision was made by an algorithm.
- Disparate impact: a business can be legally liable for discrimination even when it had no intention of discriminating.

# Artificial Intelligence in Recruitment



- New laws curtail employers using AI technology in recruitment
  - New York City measure on Automated Employment Decision Tools
    - Exception: technology must go through what is called a “Bias Audit”
  - Illinois’ Artificial Intelligence Video Interview Act



# Artificial Intelligence in Evaluations and Termination Decisions



- Can employers use Artificial Intelligence to perform managerial and supervisory functions?
  - Report productivity with AI?
  - Report safety compliance with AI?
  - Send automatic reprimands and warnings using AI?

# EEOC Initiative on Artificial Intelligence and Algorithmic Fairness



- The EEOC recently launched an initiative to ensure that the AI used in hiring and employment decisions comply with federal EEO laws. Per the EEOC, as part of the new initiative, the EEOC plans to:
  - Establish an internal working group to coordinate the agency's work on the initiative;
  - Launch a series of listening sessions with key stakeholders about algorithmic tools and their employment ramifications;
  - Gather information about the adoption, design, and impact of hiring and other employment-related technologies;
  - Identify promising practices; and
  - Issue technical assistance to provide guidance on algorithmic fairness and the use of AI in employment decisions.

# Best Practices In Using Technology To Aid Employment Decisions



- Accurate performance reviews of current workforce.
- Tell the system not things you *think* will make a hire successful but things you *know* will do so based on the people who are working for you now. That includes adding for the capture of critical soft skills.
- Data needs to be thoroughly vetted to ensure it is complete, proven, authoritative, authenticated, and from reliable sources.
- If data is drawn from questionable or unvetted sources, it should either be eliminated altogether or should be given lower confidence scores.
- Language should be as objective as possible when laying out skills and qualifications the employer is looking for.
- Data needs to be cleansed from known discriminatory practices that can skew algorithms.

# Biometric Information Privacy Laws



What does biometric privacy mean?

- The privacy of information that is “biologically unique to the individual; therefore, once compromised, the individual has no recourse...[and] is at heightened risk for identity theft.” 740 ILCS 14/5(c)
- It is the idea that individuals want their biological characteristics, including, but not limited to, fingerprints, voiceprints, palm prints, and face geometry, to be kept private to avoid identity theft and risk exposure of general personal and private biological characteristics
- Idea of an employer invading an employee’s privacy in this regard

# Biometric Information Privacy Laws



States with specific biometric privacy statutes:

- Illinois (private right of action)
- Texas (*no* private right of action)
- Washington (*no* private right of action)

# Lessons From Early Cases – Illinois BIPA



- *Rosenbach v. Six Flags Enter. Corp.*
  - Illinois employees do not have to allege actual harm to state a cause of action under IL BIPA
  - “[A]n individual need not allege some injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an ‘aggrieved’ person and be entitled to seek liquated damages and injunctive relief pursuant to [BIPA]”

# Union Employee BIPA Claims Preempted by Federal Labor Law – Illinois BIPA



- *Walton v. Roosevelt University*
  - Recent case where an Illinois appellate panel held that a union employee's claims against his employer under IL BIPA were "preempted by the Labor Management Relations Act"
  - Arguably one of the only "employer-friendly" BIPA decisions yet

# Biometric Privacy Legislation Introduced Recently In Other States:



- California Senate Bill 1189
- New York State Assembly Bill A27
- Maryland House Bill 259
- Massachusetts Senate Bill 2687
- Kentucky House Bill 626
- Maine House Bill 1945
- Missouri House Bill 2716



# Missouri House Bill 2716



- At first glance, the new Missouri bill appears to have certain similar aspects to the Illinois BIPA statute, including:
  - Must develop a written policy establishing a retention schedule and guidelines for permanently destroying biometric identifiers and information
  - Must obtain informed consent in writing that a biometric identifier or biometric information is being collected or stored
  - Must obtain informed consent of the purpose and length of term for which biometric information is collected, stored, and used

# Potential Federal BIPA Statute



- National Biometric Information Privacy Act of 2020
- Did not pass
- But could come up again in the future

# Biometric Privacy Laws – Employer Takeaways



- Under Illinois BIPA, an employer cannot collect, store, or use biometric identifiers or information for any purpose, unless the employer first:
  - Informs the employee in writing that it is collecting or storing the employee's biometric information or identifiers;
  - Informs the employee of the applicable time span and purpose for collecting, storing, and using such information; and
  - Receives a written release executed by an employee as a condition of employment.

# GPS Tracking Policies and Procedures



- How can we track our company vehicles?
- How can we keep an eye on employees' whereabouts when driving for work purposes?
- Can I track an employee's whereabouts when driving their own vehicle for work purposes?

# Company-Owned Vehicles



- Employers may have the practice or anticipate one day having the practice of installing GPS tracking devices in company-owned vehicles
- Generally, employers use tracking devices to monitor the mileage, speed, and efficiency of the employees who are driving the company-owned vehicles for work purposes

# Company-Owned Vehicles



- Minimal case law
- *Elgin v. Coca-Cola Bottling Co.* (E.D. Mo. 2005)
  - Employee sued employer based in part on an alleged violation of his rights after employer attached a GPS tracking device to employee's company van without his knowledge.
  - Court found that the installation of a GPS tracking device in a company vehicle does not constitute a tangible change in employment conditions, and that he did not suffer any adverse employment actions.

# Employee-Owned Vehicles



- Employers may have the practice or anticipate one day having the practice of installing GPS tracking devices in employee-owned vehicles, when the employee uses his or her own vehicle for work purposes.
- Although it is the employee's personally owned vehicle, an employer who approves such vehicle for work purposes may be inclined to monitor the mileage, speed, and driving efficiency of the employee for business-related purposes.

# Employee-Owned Vehicles



- *Cunningham v. New York Department of Labor* (NY Ct. App. 2013)
- Employer GPS searches outside of business hours and for non-business purposes – **must** be avoided outside of business hours and for non-business purposes
  - This is where effective company policies and procedures come into play



# GPS Tracking – Employer Takeaways



- Maintain a policy that notifies and informs employees of the employer's intended use of GPS or tracking devices
- Always obtain written consent before putting a GPS device in a company owned-vehicle or an employee-owned vehicle
  - If an employee-owned vehicle, have the employee acknowledge when the device will be active and turned on, and make sure it is not used for non-work purposes