

Practical Privacy: What Data Privacy and Artificial Intelligence Mean for Your Business and Your Employees

Presented by:

Sean C. Urich (Dallas)

Lauren N. Watson (Raleigh)



Team Members



Sean C. Urich, Esq.

sean.urich@ogletree.com

214-624-1155

8117 Preston Road, Ste. 500

Dallas, TX 75225



Lauren N. Watson, Esq.

lauren.watson@ogletree.com

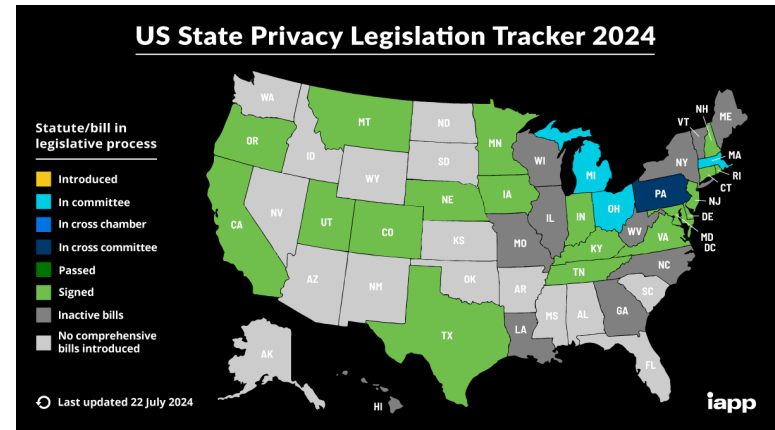
919-256-6599

8529 Six Forks Road, Ste. 600

Raleigh, NC 27615

Comprehensive Data Privacy Laws (In Effect)

- California Consumer Privacy Act
- Colorado Privacy Act
- Connecticut Personal Data Privacy and Online Monitoring Act
- Oregon Consumer Privacy Act
- Texas Data Privacy and Security Act
- Utah Consumer Privacy Act
- Virginia Consumer Data Protection Act



Comprehensive Data Privacy Laws (Impending)

- Montana Consumer Data Privacy Act (**Effective October 1, 2024**)
- Delaware Personal Data Privacy Act (Effective January 1, 2025)
- Iowa Consumer Data Protection Act (Effective January 1, 2025)
- Nebraska Data Privacy Act (Effective January 1, 2025)
- New Hampshire SB 255 (Effective January 1, 2025)
- New Jersey SB 332 (Effective January 15, 2025)
- Tennessee Information Protection Act (Effective July 1, 2025)
- Minnesota Consumer Data Privacy Act (Effective July 31, 2025)
- Maryland Online Data Privacy Act (Effective October 1, 2025)
- Rhode Island Data Transparency and Privacy Protection Act (Effective January 1, 2026)
- Indiana Consumer Data Protection Act (Effective January 1, 2026)
- Kentucky Consumer Data Protection Act (Effective January 1, 2026)

Comprehensive Data Privacy Laws – High Points

- California – the only comprehensive privacy law applying to employee data (so far!)
- Notice at Collection
- Contractual restrictions with service providers
- Procedures for honoring opt-out rights and other data subject rights
- Data protection assessments
- Restrictions around the collection/use/opt-out for “sensitive data”
- Restrictions on the use of artificial intelligence in decisionmaking

Notice at Collection and Data Subject Rights

Notice at Collection

- What personal information is being collected?
- How are you collecting it?
- How are you using it?
- Are you sharing (disclosing) it with anyone?
- Are you selling it or using it for targeted advertising purposes?
- How are you safeguarding the data?
- How long do you retain the data?



Notice at Collection and Data Subject Rights

Data Subject Rights

- Vary from jurisdiction to jurisdiction, but generally include:
 - Right to Know/Access
 - Right to Deletion
 - Right to Correct
 - Right to Opt-Out of the use of personal information for targeted advertising
 - Right to Portability
 - Right to Appeal (Less Common)



Employee Monitoring Laws

Types of Employee Monitoring

- GPS or Geolocation
- Email, Keylogging, Internet Searches
- Video/Audio Surveillance
- Monitoring software that combines with AI



Employee Monitoring Laws

State Laws

- Connecticut - Notice may be in the form of a prominently displayed and easily accessible written policy that states the types of electronic monitoring that may occur in the workplace.
- Delaware - Notice may be given in writing, in an electronic record, or other electronic form, and be acknowledged by the employee in writing or electronically.
- New York - Notice must be in writing, in an electronic record, or in another electronic form and must be acknowledged by the employee either in writing or electronically. Employer must post a notice in a conspicuous place that is readily available for viewing.

Employee Monitoring Laws



© 2024, Ogletree, Deakins, Nash, Smoak & Stewart, P.C.

Other Considerations

- State and federal wiretapping laws
- National Labor Relations Act
- Privacy Common Law – Tort of Invasion of Privacy
- Federal Laws (Computer Fraud and Abuse Act, Wiretap Act, Stored Communications Act)

Employee Monitoring Laws

Best Practices

In all states, it is a best practice to have the below pieces in place before using employee monitoring technologies:

- Policy
- Notice
- Consent



Employee Monitoring Laws

Have you integrated artificial intelligence in your day-to-day business operations?



Artificial Intelligence in the Workplace – Common Tools

- **Resume Scanners** – identifying keywords to prioritize certain applications
- **Employee Monitoring** – employees are rated on things like keystrokes and other factors
- **Chatbots** – providing 24/7 support to employees, including answering questions and identifying and linking documents
- **Video Interviewing** – evaluating candidates based on things like facial expressions and speech patterns
- **AI Notetakers** – transcribing meetings, including through the use of voice recognition technologies, creating and organizing notes of meetings



Artificial Intelligence in the Workplace – Common Tools

What AI tools is your organization using?



Artificial Intelligence in the Workplace – Considerations for the Use of Common Tools in the Employment Context

Considerations arise at both the federal and state levels:

- NLRB
- EEOC
- Executive Orders
- State and Local Laws



National Labor Relations Board

10/22 General Counsel Memo:

- Non-binding enforcement position
- Focused on electronic monitoring, algorithmic management, and violations of Section 7 rights.
- Identifies *existing violations plus proposed new standard*.
- Review in conjunction with all policies and new technology.



National Labor Relations Board – General Counsel Memo

Existing Violations:

- Failure to bargain in organized workplace.
- Using technology to obtain information regarding PCA.
- Instituting new technology in response to PCA.
- Buying social media to monitor information regarding PCA.
- Using technology to preclude PCA.
- Using AI to screen out those likely to engage in PCA.

National Labor Relations Board – General Counsel Memo

Proposed New Standard:

- Employer presumed to violate 8(a)(1) if “surveillance and management practices, viewed as a whole . . . tend to interfere with or prevent a reasonable employee from engaging in [protected activity].”
- Narrowly tailored practices with legitimate business need – i.e., needs that can’t be met through less damage to employee rights.

EEOC Guidance

EEOC Guidance Issued 5/22:

- Guidance focuses on disability related inquiries
- Employer liable for vendor / third-party Automated Decision-Making Tool (ADT), even where the system is designed or administered by someone else
- ADT must be accessible (reasonable accommodations required)
- ADT can't "*screen out*" individuals with disabilities, including by using tools that prevent an applicant from meeting or lower their performance on selection criteria

EEOC Guidance

“Promising Practices”:

- Clear instructions on requesting accommodations
- Explanations of the metrics measured by ADT, how they are measured, and whether a disability may lower an assessment
- Assessing whether the ADT disadvantages disabled individuals.
- Ensuring the ADT interface is accessible to disabled individuals.
- Alternative formats or assessments for disabled individuals.

EEOC Guidance

EEOC Guidance Issued 5/23:

- Focused on disparate impact in selection procedures (hiring/firing/promotion).
- Reemphasizes employer liability for vendor / 3rd party ADT even where the employer is assured by vendor assessments there will be no adverse impact.
- Employers should self-audit ADT at start of use and on an on-going basis.
- 4/5ths rule of Uniform Guidelines on Employee Selection Procedures is a “rule of thumb” but not determinative.

Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

- The EO directed a number of actions across the federal and privacy spheres. Relevant to the employment space, the EO called for the development of principles and best practices to benefit workers:
- In response, the DOL developed the following AI Principles for Developers and Employers:
 - **Centering Worker Empowerment:** Workers and their representatives, especially those from underserved communities, should be informed of and have genuine input in the design, development, testing, training, use, and oversight of AI systems for use in the workplace.
 - **Ethically Developing AI:** AI systems should be designed, developed, and trained in a way that protects workers.
 - **Establishing AI Governance and Human Oversight:** Organizations should have clear governance systems, procedures, human oversight, and evaluation processes for AI systems for use in the workplace.
- **Ensuring Transparency in AI Use:** Employers should be transparent with workers and job seekers about the AI systems that are being used in the workplace.
- **Protecting Labor and Employment Rights:** AI systems should not violate or undermine workers' right to organize, health and safety rights, wage and hour rights, and anti-discrimination and anti-retaliation protections.
- **Using AI to Enable Workers:** AI systems should assist, complement, and enable workers, and improve job quality.
- **Supporting Workers Impacted by AI:** Employers should support or upskill workers during job transitions related to AI.
- **Ensuring Responsible Use of Worker Data:** Workers' data collected, used, or created by AI systems should be limited in scope and location, used only to support legitimate business aims, and protected and handled responsibly.

State and Local AI Guidance

- Illinois and Maryland have laws governing employer use of AI in video interviews. These require certain notices and, in Illinois, reporting to the state government.
- New York City Local Law 144 restricts employer use of AI technologies, by prohibiting the use of automated employment decision tools unless certain requirements (including the completion of a bias audit) are met.
- Colorado and Utah have passed broader artificial intelligence laws in the past year that, while not entirely focused on employers, will nevertheless have an impact on business operations.

Artificial Intelligence in the Workplace – AI & Biometrics

The use of artificial intelligence tools in the workplace often involves the collection of and use of biometric information.

- Biometric information is generally described as a person's unique biological or behavioral characteristics that can be used to identify the person.
- Biometric information is often collected using the following, potentially AI equipped tools:
 - DashCam devices – MV+AI technology; camera allegedly scans drivers' facial geometry
 - "Talkman" headsets – MV+AI technology used to pick orders; allegedly collects voiceprints
 - Security cameras – allegedly scan facial geometry

Artificial Intelligence in the Workplace – AI & Biometrics

State Biometric Privacy Laws

- Illinois
- Texas
- Washington
- Colorado (Effective July 1, 2025)

Other Considerations

- FTC Biometric Privacy Memo and DPIA Expectations
- NLRB

Artificial Intelligence in the Workplace – AI & Biometrics

Have you implemented any AI-specific policies to govern or restrict the use of AI technologies?



Artificial Intelligence in the Workplace – AI & Biometrics



Are you training your employees on acceptable and unacceptable uses of AI tools in the workplace?

Artificial Intelligence in the Workplace – Mitigating Risk

Know your tools and vendors

- Carefully vet new technology and devices for artificial intelligence and biometric capabilities (and vet whether litigation is underway)
- Ensure new vendors are well-established and negotiate indemnification and hold harmless clauses in vendor contracts

Artificial Intelligence in the Workplace – Mitigating Risk

Set expectations and train employees

- Prepare policies to describe appropriate and inappropriate uses of artificial intelligence in your workplace.
- Set employee expectations regarding the use of AI tools and the consequences of misusing these tools.
- Train your employees on acceptable use of AI tools.



shutterstock.com · 2473571595

Artificial Intelligence in the Workplace – Mitigating Risk



.... And do it again!

- Review your policies on at least an annual basis
- Monitor the legal landscape associated with AI tools (especially those that involve the use of biometric information) and revise your policies as needed to maintain compliance.



Sean C. Urich, Esq.

sean.urich@ogletree.com
214-624-1155
8117 Preston Road, Ste. 500
Dallas, TX 75225



Lauren N. Watson, Esq.

lauren.watson@ogletree.com
919-256-6599
8529 Six Forks Road, Ste. 600
Raleigh, NC 27615