The Intersection of AI, Employment Law, and Compliance: Preparing for What's Next

Presented By:

John Carrigan, Jr.
Jeffrey Klamut
Cozen O'Connor
January 2026

COZEN O'CONNOR

Agenda

- AI Orientation
- AI Regulations
- AI Legislation
- AI Compliance Tips

AI Orientation

Lorem ipsum

WHAT are we talking about?

- **Artificial Intelligence (AI):**

"An engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments."

-- California AI Transparency Act, Artificial Intelligence Training Data Transparency Act, Transparency in Frontier AI Act

"A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to –
(A) perceive real and virtual environments;
(B) abstract such perceptions into models through analysis in an automated manner; and
(C) use model inference to formulate options for information or action."
- National Artificial Intelligence Initiative Act of 2020

"An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment."

***- Organisation for Economic Co-operation and Development Definition* (Mar. 2024)**

WHAT are we talking about?

- **Generative AI:**
  - **"[A]rtificial intelligence that can generate derived synthetic content, including text, images, video, and audio, that emulates the structure and characteristics of the system's training data."**

    California AI Transparency Act

  - **"[A] category of AI that can create new content such as text, images, videos, and music."**

    OECD definition

  - **AI that is "designed to mimic the structure and characteristics of input data to generate outputs such as text, sound, images, videos, and other creative content."**

    South Korea AI Basic Act

WHERE are we?

Nov 2022	OpenAI launches ChatGPT
Mar–Apr 2023	Microsoft, Google, Meta, and Anthropic debut AI products
Oct 2023	President Biden signs Executive Order on AI (EO 14110)
Mar 2024	European Parliament adopts EU AI Act
May 2024	Colorado enacts AI Act
Aug 2024	Illinois amends Human Rights Act to regulate ADMT
Sep 2024	California Gov. signs 18 laws but vetoes Safety Bill
Dec 2024	South Korea passes AI Basic Act
Jan 2025	Executive Order 14110 repealed
Feb 2025	EU ban on Prohibited AI effective
Apr 2025	OMB memos on AI released
May 2025	Japan enacts AI Promotion Act
Jun 2025	Texas enacts TRAIGA CA Civil Rights Council Approves ADS regs
Jul 2025	President Trump issues America's AI Action Plan
Sep 2025	CPPA regulations for ADMT approved California passes TFAIA
Oct 2025	CA ADS regs effective
Dec 2025	Vietnam passes Law on Artificial Intelligence President Trump signs Executive Order 14365 NY passes RAISE Act South Korea amends AI Basic Act

Timeline of major AI governance developments from ChatGPT launch through December 2025

COZEN O'CONNOR

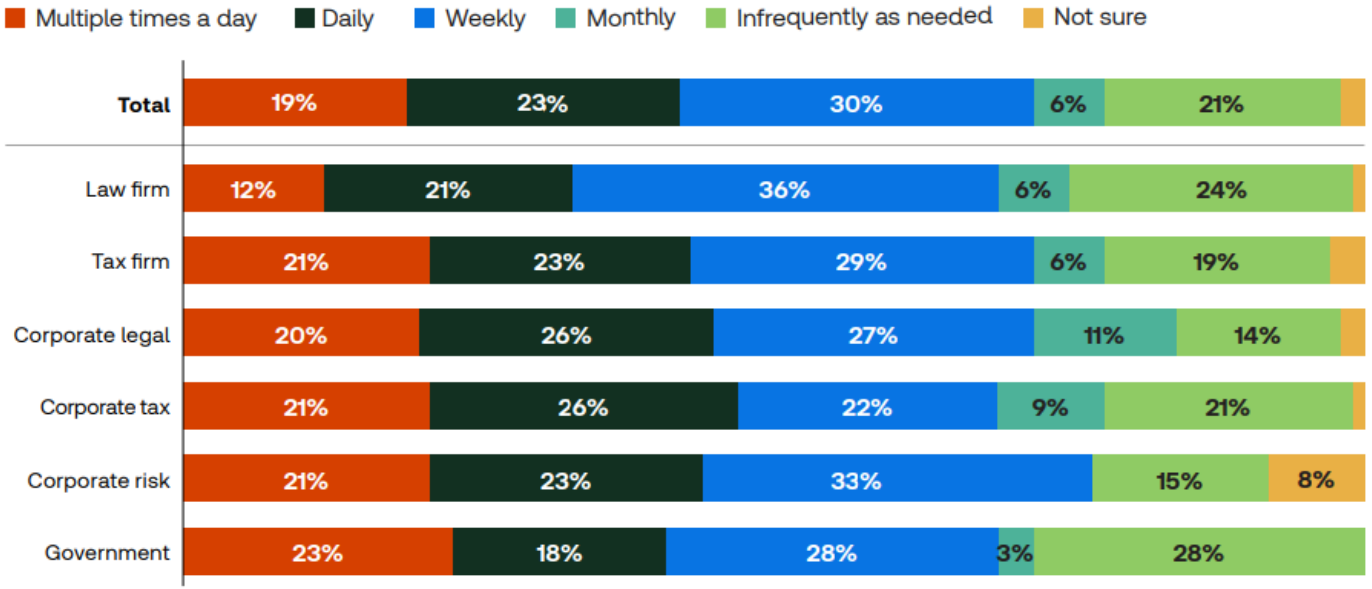
WHO is using AI?

- **Professional Services**: **Professionals who said their organizations were actively using GenAI *nearly doubled* over the past year, to 22% in 2025, compared to 12% in 2024.**

2024 Generative AI in Professional Services, Thomson Reuters Institute, available at: https://www.thomsonreuters.com/content/dam/ewp-m/documents/thomsonreuters/en/pdf/reports/2025-generative-ai-in-professional-services-report-tr5433489-rgb.pdf

FIGURE 16:

Frequency of GenAI use among current users



Source: Thomson Reuters 2025

Risks of Using AI

- **Confidential and Proprietary Information Leaks**
  - Amazon (January 2023), Samsung (May 2023).
- **Security Vulnerabilities**
  - AI systems can be vulnerable to adversarial attacks. Generative AI models can create convincing social engineering attacks, including phishing and deepfake media.
- **Accuracy**
  - Generative AI systems deliver polished outputs that can promote a false sense of accuracy. Cases of professionals mistakenly relying upon inaccurate or fabricated information from AI continue to abound.
  - The accuracy of a generative output can be limited by that of the input and/or prompt.
- **Ethical Concerns**
  - AI, particularly GenAI, raises concerns about data collection, use, and retention by AI systems and users; how models are trained on data (and resulting biases are created); how outputs are used and who owns them; human oversight; and transparency.

Risks of AI In-House (continued)

- **Employee Data Privacy and Confidentiality**
  - If employee data is inputted to an AI system without adequate security protocols (or used to train an AI without adequate anonymization), it could lead to unauthorized data exposure, data exfiltration, or even identity theft.
- **Disparate Impact and Unintentional Bias**
  - An AI system trained on intentionally or unintentionally biased data could favor certain demographics over others. *See Mobley v. Workday*, 3:23-cv-00770-RFL (N.D. Cal) (now a collective action alleging disparate impact in AI hiring).
  - AI has potential to produce skewed results from additional phenomena, such as overfitting, inappropriate focus, and interpretive bias.
- **Job Displacement and Workforce Impact**
  - AI may reduce the need for certain entry-level roles, leading to layoffs and potential reputational risks for a deploying company.

- ***Mobley v. Workday, Inc.(N.D. Cal. 2023):***
  - **On May 16th, 2025, the Court granted conditional certification for the case to proceed as a nationwide collective action under the Age Discrimination in Employment Act (ADEA).**
  - **The Court rejected Workday's argument that it is just a software provider and does not make the hiring decisions, finding Workday sufficiently involved in the hiring process to be held potentially liable as an 'agent' of the employers.**

- ***Harper v. Sirius XM Radio, LLC (E.D. Mich. 2025):***
  - **On August 4, 2025, plaintiff filed a class action complaint alleging that Sirius' use of a commercial AI hiring tool that screens and analyzes resumes resulted in racial discrimination against him and other similarly situated African American applicants.**

AI Regulations

Lorem ipsum

California Civil Rights Council Regulations

Effective 10/1/2025

- **What employers do these regulations apply to?**
  - **Employers of 5 or more people, employment agencies, unions, apprentice programs**
    - **Includes PT employees, employees on leave; inside/outside California**
    - **Employer Agents - any person acting on behalf of an employer, directly or indirectly, to exercise a function traditional exercised by the employer- are also an "employers."**
- **What is an Automated-Decision Systems ("ADS")?**
  - **An ADS is "[a] computational process that makes a decision or facilitates human decision making regarding an employment benefit," including processes that "may be derived from and/or use artificial intelligence, machine-learning, algorithms, statistics, and/or other data processing techniques."**

Civil Rights Council Regulations (cont'd)

Examples of ADS Use In Employment Settings

- **Using computer-based assessments or tests, such as questions, puzzles, games, or other challenges to:**
  - **Make predictive assessments**
  - **Measure skills, dexterity, reaction-time, and/or other abilities or characteristics;**
  - **Measure personality traits, aptitude, attitude, cultural fit;**
  - **Screen, evaluate, categorize, make recommendations**
- **Screening resumes for particular terms or patterns**
- **Directing job advertisements or other recruiting materials to targeted groups**
- **Analyzing facial expression, word choice, and/or voice in online interviews**
- **Analyzing employee or applicant data acquired from third parties**

Civil Rights Council Regulations (cont'd)

- **What Conduct is Targeted?**
  - Using ADS or selection criteria (including a qualification standard, employment test, or proxy) to discriminate based on a protected class.
  - Using ADS to engage in unlawful recruitment practices (e.g., to restrict, exclude, or classify individuals on a protected trait; to engage in unlawful preemployment inquiries, including criminal history).
  - Using ADS to screen based on disability, uncorrected vision or hearing, unless:
    - The standard, test, or selection criteria is job related and consistent with business necessity.
    - There is no less effective discriminatory standard, test or other selection criteria.
  - Expressing a preference for or advertising employment availability or benefits in a manner intended to discriminate based on a protected trait.
  - To conduct an unlawful "medical or psychological examination"
  - To aid or abet unlawful employment discrimination.

Civil Rights Council Regulations (cont'd)

- **Who Can Be Responsible?**
  - Employers, whether they use their own AI tools or use a third parties AI tools.
  - Third parties that design or implement such AI tools may also be held liable under the FEHA's prohibition on aiding and abetting unlawful employment practices .

- **Are there New Recordkeeping requirements?**
  - Yes. Employers must keep for four years all automated-decision system data created or received by the employer or other covered entity dealing with any employment practice and affecting any employment benefit of any applicant or employee.
    - Keep for four years (up from two) from the date of the making of the record or the date of the personnel action involved, whichever occurs later.
    - Includes all applications, personnel records, membership records, employment referral records, California employment information reports, selection criteria, automated-decision system data, and other records created or received by the employer or other covered entity dealing with any employment practice and affecting any employment benefit of any applicant or employee.

Civil Rights Council Regulations (cont'd)

- **What you need to do:**
  - **Identify all AI and ADS tools used in the employment relationship and audit to ensure compliance with antidiscrimination laws.**
  - **Review vendor relationships and make sure contracts include requirements for transparency, bias testing, data retention and cooperation with audits.**
  - **Update policies and processes and integrate AI governance as appropriate**
  - **Ensure that all ADS-related systems include mechanisms for applicants to request accommodations for disabilities, religious practices, or medical conditions.**
  - **Update retention policies to ensures that all ADS-related employment data is retained for the required four years.**
  - **Train HR, managers, recruiters and others on AI and the new regulations.**

STAY INFORMED AND UP-TO-DATE

California Consumer Privacy Act Regulations

Effective 1/1/2027

- **Apply to:**
  - **Businesses subject to the CCPA that use automated decision-making technology ("ADMT") to**
    - **Make a "significant decision" concerning a consumer**
      - That results in the provision or denial of certain services and opportunities, including employment or independent contracting.
        - » **Hiring**
        - » **Work allocation/assignment of employees; compensation, incentive compensation (e.g., bonuses), or other benefits ("Allocation")**
        - » Promotion, demotion, suspension, and termination
    - **Conduct "extensive profiling"**
      - includes analyzing personality, interests, behavior, or location in their workplace or to target ads to them
    - **Train ADMT that can**
      - Identify people (e.g., facial-recognition technology);
      - Profile people (e.g., using personal information to evaluate a person's ability, traits, preferences, etc.);
      - Make significant decisions; or
      - Generate synthetic media (e.g., images of real people that are presented as truthful or authentic).

California Consumer Privacy Act Regulations (cont'd)

ADMT

"[A]ny technology that processes personal information and uses computation to replace human decisionmaking or substantially replace human decisionmaking."

ADS does not include:

"web hosting, domain registration, networking, caching, website-loading, data storage, firewalls, anti-virus, anti-malware, spam- and robocall-filtering, spellchecking, calculators, databases, and spreadsheets, provided that they do not replace human decisionmaking"

.

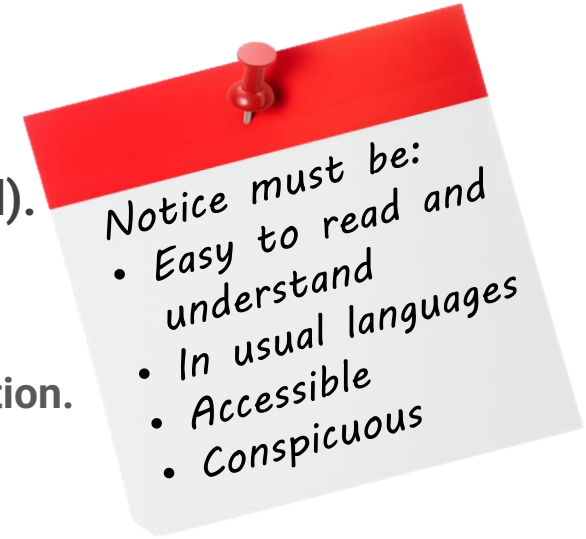
Substantially replace

Using the technology's output to make a decision without human involvement. Human involvement requires the human reviewer to:

- **Know how to interpret and use the technology's output to make the decision;**
- **Review and analyze the output of the technology, and any other information that is relevant to make or change the decision;**
- **Have the authority to make or change the decision based on their analysis.**

California Consumer Privacy Act Regulations (cont'd)

- **New Obligations:**
  - **Provide a Pre-Use Notice, containing:**
    - The specific purpose for using use the ADMT (generic terms not allowed).
    - Notice of the right to opt-out of ADMT and how to opt-out (with link), or
      - If opt-out is not required due to human appeal exception: how to appeal
      - If opt-out is not required due to other exceptions, identification of the exception.
    - A description of the consumer's right to access their ADMT data
    - Notice on non-retaliation
    - Additional information re: how the ADMT works:.
      - How ADMT processes personal information (including categories that affect the ADMT's output).
      - The type of output generated by ADMT and how it is used to make a significant decision
        - » Whether the output is the sole factor or whether other factors are considered
        - » If there is no "human involvement," the roles of any humans in the decisionmaking process
        - » The alternative process for making a significant decision who consumers who opt-out



California Consumer Privacy Act Regulations (cont'd)

- **Meet Opt-Out or Opt-Out Exception Requirements:**
  - **A business must provide consumers with an easy way to opt-out of the use of ADMT, except**
    - **If there is a Human Appeal**
      - **The business provides the consumer with a method to appeal the decision to a human reviewer with ability to review the ADMT output and authority to overturn the significant decision.**
      - **The human reviews and analyzes the ADMT's output and "any other information that is relevant to change the significant decision at issue."**
      - **The human considers information provided by the consumer in support of their appeal and may consider other sources of information.**
      - **The business clearly describes to the consumer how to submit an appeal and enable the consumer to provide supporting information to the human reviewer.**
    - **If the ADMT is used for Hiring/Admission and Allocation**
      - **ADMT must be used solely for the intended purpose and must actually work for the purpose**
      - **ADMT must not unlawfully discriminate on the basis of protected traits.**

California Consumer Privacy Act Regulations (cont'd)

- **Comply with Requests to Access/Appeal ADMT:**
  - **Timing:** 10 business days to confirm, 45 (extendable to 90) calendar days to respond.
  - **Responses to requests to access: Plain explanation of**
    - Specific purpose for using ADMT (not generic)
    - Information about the ADMT's logic explaining how ADMT processed their personal information to generate an output about them.
      - » Parameters that generated the output
      - » The specific output
    - The outcome of the decisionmaking process for the consumer
      - » Whether output was the sole factor to make the decisions
      - » If no, which other factors played a role in the decision
      - » If there is no "human involvement," the roles of any humans in the decisionmaking process
      - » How, if at all, the output will be used to make future significant decisions about the consumer
    - Non-retaliation rights
  - **Limitations:** the response does not need to contain trade secrets or certain information that compromise business' safety/security practices.

California Consumer Privacy Act Regulations (cont'd)

A business's response to a consumer's access request would have to include:

- Why the business used the ADMT;
- How the ADMT worked with respect to that consumer, such as the key factors that affected the ADMT's output and what the output was; and how the business used the output to make a decision about that consumer.
  - *For example, if a business used emotion-assessment technology during a job applicant's interview to score their predicted performance at work and then used that score to decide whether to hire that applicant, the business would give that consumer's score and explain how the score factored into the business's decision to hire them; and*
- How the consumer could exercise their other CCPA rights (e.g., their right to correct inaccurate information), and that the business cannot retaliate against them for exercising their rights.

Source: https://cppa.ca.gov/meetings/materials/adt_regulations.pdf

California Consumer Privacy Act Regulations (cont'd)

- **Update Privacy Policy to include:**
  - Disclosures about use of ADMT and opt-out rights, as applicable.
  - Notice of right to access ADMT
  - Notice of non-retaliation
  - How to request and access ADMT
- **Update risk assessment process:**
  - Risk assessments due 12/31/2027, first attestations 4/1/2018
  - Then every time before new ADS, every 3 years, and 45 days after substantial change
  - Must explain, among other things:
    - A description of the ADMT's purpose,
    - Data categories, processing methods, retention periods, disclosures, third-party involvement
    - The benefits and potential negative impacts of using the ADMT, the
    - The safeguards implemented to mitigate those negative impacts.
  - Must involve individuals who are processing personal information
  - Must be certified by a qualified executive.

California Consumer Privacy Act Regulations (cont'd)

- **Takeaways for HR/Employers Using / Planning to Use ADS**
  - **Understand the types of employment decisions for which ADS is used**
    - This is relevant to opt-out rights and ensuring data collections are tailored to intended use
  - **Prepare for pre-use notices**
    - Understand how ADMT will collect, process, and output data for each use case
    - Understand/determine scope of human involvement, appeal
    - Determine whether use cases fall under opt-out exception
  - **Map responsibilities to appropriate stakeholders**
  - **Prepare processes for**
    - Opt-out process, if applicable
    - Human appeal
    - Requests for access
    - Risk assessments (reference: ISO/IEC 42005:2025 – AI System Impact Assessment)
  - **Update policies**

AI Legislation in California and Beyond

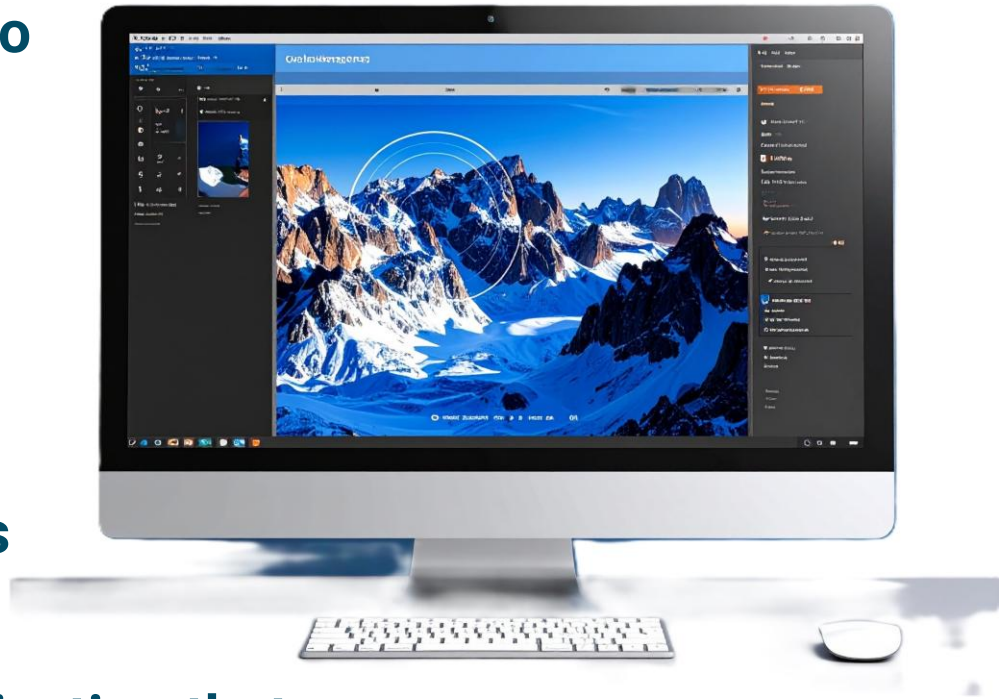
- AI Transparency Act (SB 942)
  - Bus. & Prof. Code § 22757, *et seq.*
  - Effective 1/1/2026
- Generative AI Data Transparency Act (AB 2013)
  - Civ. Code § 3110, *et seq.*
  - Effective 1/1/2026
- Transparency in Frontier AI Act (SB 53)
  - Bus. & Prof. Code § 22757.10 *et seq.*; Lab. Code § 1107 *et seq.*; Gov't Code § 11546.8
  - Effective 1/1/2026
- Additional Laws

AI Transparency Act (SB 942, eff 1/1/2026)

- **Applies to:**
  - **Covered Providers: producers of large GenAI systems**
    - System must have over 1,000,000 monthly visitors or users and be publicly accessible within the geographic boundaries of California
  - **Licensees of large AI systems**
- **Obligations for Covered Providers:**
  - **Offer a "manifest disclosure" in GenAI image, video, or audio content**
    - Clearly identifies content as AI generated and is "extraordinarily" hard to remove
  - **Include a "latent disclosure" in GenAI image, video, or audio content**
    - Identifies the covered provider, GenAI system and version, timestamp, and unique ID
  - **Provide an "AI Detection Tool" at no cost to user, to reveal latent disclosures**
  - **Require licensees (by contract) to maintain the system's latent disclosure capability and revoke license to those who breach such provisions**

AI Transparency Act (cont'd)

- **Obligations for Licensees:**
  - Do not tamper with covered provider's ability to maintain latent disclosures in GenAI content
  - Stop using GenAI system if license is revoked
- **Violations:**
  - Enforced by AG, county, or city counsel
  - Covered entities: $5,000 per day
  - Licensees: injunctive relief and attorneys' fees
- **Exceptions:**
  - Any product, service, internet website, or application that provides exclusively non-user-generated video game, television, streaming, movie, or interactive experiences.



GenAI Data Transparency Act (AB 2013 eff 1/1/2026)

- **Applies to:**
  - Developers: anyone who designs, codes, produces, or substantially modifies an AI system or service for use by members of the public.
  - Any GenAI system (or substantial modification thereof) that is publicly released after 2022 to Californians, either free or paid.
- **Obligations:**
  - Developer must post on their website a high-level summary of datasets used to develop the GenAI system

Who own datasets?	How many datapoints?	Copyrighted/TM material?	Include personal information?
Their purpose?	Datapoint types?	Licensed/paid for?	Consumer data?
When collected?	When first used?	Synthetic data used?	Was data sanitized?

- **Violations:** Nothing explicit in Act, but will be enforced under California UCL.

Transparency in Frontier AI Act (SB 53, eff 1/1/2026)

- **Applies to:**
  - **Frontier Developers: Anyone who trains a large foundation model using certain levels of compute for the training, fine tuning and modification processes.**
  - **Large Frontier Developers: A frontier developer with >$500M annual revenue.**
- **Obligations for Frontier Developers:**
  - **Publish a transparency report containing website, contact info, release date, languages supported, output modalities, intended use, and terms of use.**
  - **Report critical safety incidents to California's Office of Emergency Services within 15 days (or 24 hours if imminent risk of death/injury).**
  - **Cannot retaliate for or prohibit employees disclosing actions that pose a specific and substantial danger to the public health or safety resulting from a catastrophic risk, or a violation of the Act.**
  - **Notify employees, through posting or annual notice of whistleblowing rights.**
  - **No materially false/misleading statements about catastrophic risks.**

Transparency in Frontier AI Act (cont'd)

- **Obligations For Large Frontier Developers:** ***All obligations for Frontier Developers****, plus:*
  - **Add summary of catastrophic risk assessments and results to transparency report**
  - **Provide anonymous reporting hotline to employees, monthly investigation update to whistleblower, and report results to officers/directors**
  - **Provide regular catastrophic risk disclosures to the OES**
  - **Create, publish, follow, and annually update an AI Frontier Framework:**

Internal governance, int'l standards and best practices	**How catastrophic risk potential is assessed**	**Risk mitigation efforts and review thereof**	**Third party risk assessments**
When to update framework and disclosures	**Managing internal catastrophic risk**	**Identifying/responding to critical safety issues**	**Cybersecurity**

  - **No materially false/misleading statements about compliance**
- **Violations:**
  - **Up to $1M per violation of Act (enforced by AG)**
  - **Private right of action for whistleblower violations**

Additional California AI Laws

- **SB 253:** Regulations for AI "Companion Chatbots" including initial notice and every 3 hours later that chatbot is not human, protocol to address suicidal ideations from users, posting requirements, audits, and private rights of action.
- **AB 1008:** Amends CCPA to state that AI systems can disclose Personal Data
- **AB 2602:** Creates contractual protections around using AI-generated digital replicas of a living performer's voice or likeness
- **AB 1836:** Requires consent for using AI-generated digital replicas of a deceased individual's voice or likeness
- **SB 926:** Criminalizes the creation and distribution of nonconsensual, sexually explicit deepfakes
- **SB 981:** Requires social media platforms to enable users to report sexually explicit digital identity theft.

Other AI Laws that may affect employers

- Colorado AI Act (eff. 6/30/2026). Colo. Rev. Stat. § 6-1-1701.
  - Regulates use of high-risk AI systems in consequential employment decisions like hiring and promotion, includes transparency, risk management, and bias assessment rules
- Illinois Human Rights Act Amendments (eff 1/2026)
  - Requires notification of use of AIS for employment-related decisions
- New York
  - NYC Local Law144: ADMT use that "substantially assists or replaces" human decisions
  - RAISE Act (eff 1/1/2027) requires large AI devs to provide notice of rights to employees
- Texas Responsible AI Governance Act (H.B. 149, eff. 1/2026)
  - Regulates certain AI use of companies and gov't, prohibits intentional discrimination
- Utah AI Policy Act (2024R Utah S.B. 149)
  - Implements transparency requirements for some commercial uses of interactive AI
- The EU AI Act (rolling effective dates)
  - Risk-based approach to regulating AI by companies that touch the EU market. Unacceptable use cases, including emotion recognition at work, already banned.

U.S. Federal AI Policy

- **The U.S. Does Not Have Comprehensive Federal AI Legislation.**
  - **Ensuring a National Policy Framework for Artificial Intelligence (EO 14365, 12/11/25)**
    - National policy to promote "minimally burdensome" federal framework
    - Directs AG to form Task Force to challenge onerous state AI laws that "stymie innovation"
  - **America's AI Action Plan (7/23/25): Basic policy focused on Accelerating AI innovation, building American AI infrastructure, and leading in international AI diplomacy and security**
  - **OMB memos (4/3/25)**
    - M-25-21: *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust*
    - M-25-22: *Driving Efficient Acquisition of Artificial Intelligence in Government*
    - **Keys for businesses:**
      - Preference for U.S.-made AI programs, interoperable programs, certain contractual terms:
      - Government retains rights to its data and any improvements to that data
        - » Data is protected from unauthorized disclosure or use, and from being used to train or improve the functionality of the vendor's model without express permission.
        - » Vendor lock-in should be prevented.
      - Providing access to the underlying AI source code, models, or data, will help an agency comply with its pre-deployment testing obligations.

AI Compliance Tips

Tips For Compliance

- **Inventory how your organization is using AI.**
  - **Which tools are officially *allowed*?**
  - **Which tools are employees *actually using*?**
  - **Are you using AI for significant decisions (hiring, work allocation, comp, benefits)**
    - **If so, how?**
    - **Is there human oversight?**
- **Gain basic understanding of your AI systems' architecture.**
  - **What are the main components and how do they interact with each other?**
  - **Where is your data and how is it collected and processed?**
  - **What hardware or software is used and how is it protected?**
- **Determine which laws apply (California and beyond).**
- **Determine if any industry-specific guidelines apply to your business or role.**
  - **E.g., ABA's Model Rules, NAIC AI Principles, DOD's RAI.**

Tips For Compliance (cont'd)

- **Understand fundamental security concepts.**
  - **No Training: Is your organization's data being used to train the AI model?**
  - **Zero Day Retention: Is your AIS provider retaining inputs/outputs?**
  - **Data Minimization: Only collect and retain the data that is absolutely necessary for the AI system's function, thereby reducing the risk of exposure.**
- **Become familiar with the major risk management frameworks.**
  - **NIST AI Risk Management Framework (AI RMF 1.0)**
  - **ISO/IEC 42001:2023, an int'l standard focusing on ethics and risk management**
  - **NIST Generative AI Profile (NIST AI 600-1)**
  - **ISO/IEC 23894:2023, guidance for managing lifecycle of AI systems risks**
- **Identify prohibited and encouraged use cases and how to monitor them.**
  - **"Public AI" vs. "Enterprise AI"**
- **Develop compliance plan (including policy) tailored to applicable laws and train.**

AI Policy Tips

- **Establish the scope and relevant definitions**
  - **Policies may change depending on where they apply and who they cover so defining scope (particularly user vs. developer) is important.**
  - **Work through how concepts of AI, GenAI, Permitted AI, and Prohibited AI will interplay in your organization so that you know which terms you want to define and how. This is not "one size-fits all."**
- **State General Principles**
  - **Stating principles can fill-in any gaps and help align with risk management frameworks or industry-specific objectives.**
  - **Examples: fair, accountable, transparent, safe/secure, etc.**
- **Establish key stakeholders and decisionmakers for AI governance, accountability, and responsibility mapping.**

AI Policy Tips

- **Establish procedures for the scope of covered activities.**
  - **Incorporate relevant existing policies and procedures.**
  - **Using AI**
    - Explain the generally permitted and prohibited use cases.
    - Address any specific use cases that may require special attention (e.g., customer data, employee data, AI decision-making, etc.).
    - Provide examples or an appendix of approved AI systems.
    - Establish employee responsibilities for inputs, outputs, monitoring, and reporting.
  - **Developing AI**
    - State whether your organization intends to generally follow any relevant frameworks.
    - Cover data/model documentation, risk reviews, testing, training, and monitoring.
- **Include a reporting mechanism (e.g., ethics hotline).**
- **Allow for variability and iterative modification.**

QUESTIONS?

Lorem ipsum