PROGRAM MATERIALS
Program #36163
June 22, 2026

Legal Challenges in Automating Recruitment and Employment Practices

- Julia Jacobson, Esq. - Squire Patton Boggs
- Faye Ricci, VP, DGC- Boeing Employees' Credit Union

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 150, Boca Raton, FL 33487
Phone 561-241-1919

SQUIRE PATTON BOGGS

Legal Challenges in Automating Recruitment and Employment Practices

June 22, 2026
12:00-1:00 PM MDT

Speakers

Julia Jacobson

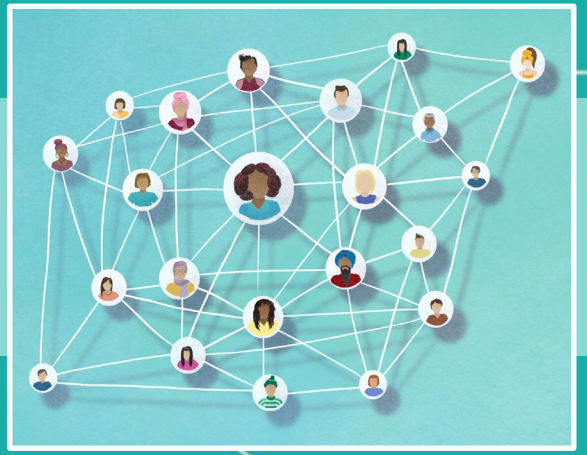
Partner, Data Privacy, Cybersecurity & Digital Assets
Squire Patton Boggs
New York
julia.jacobson@squirepb.com

Faye Ricci

VP & Deputy General Counsel - AI, Data Privacy and Contracts
Boeing Employees' Credit Union (BECU)

SQUIRE PATTON BOGGS

Introduction



Artificial Intelligence

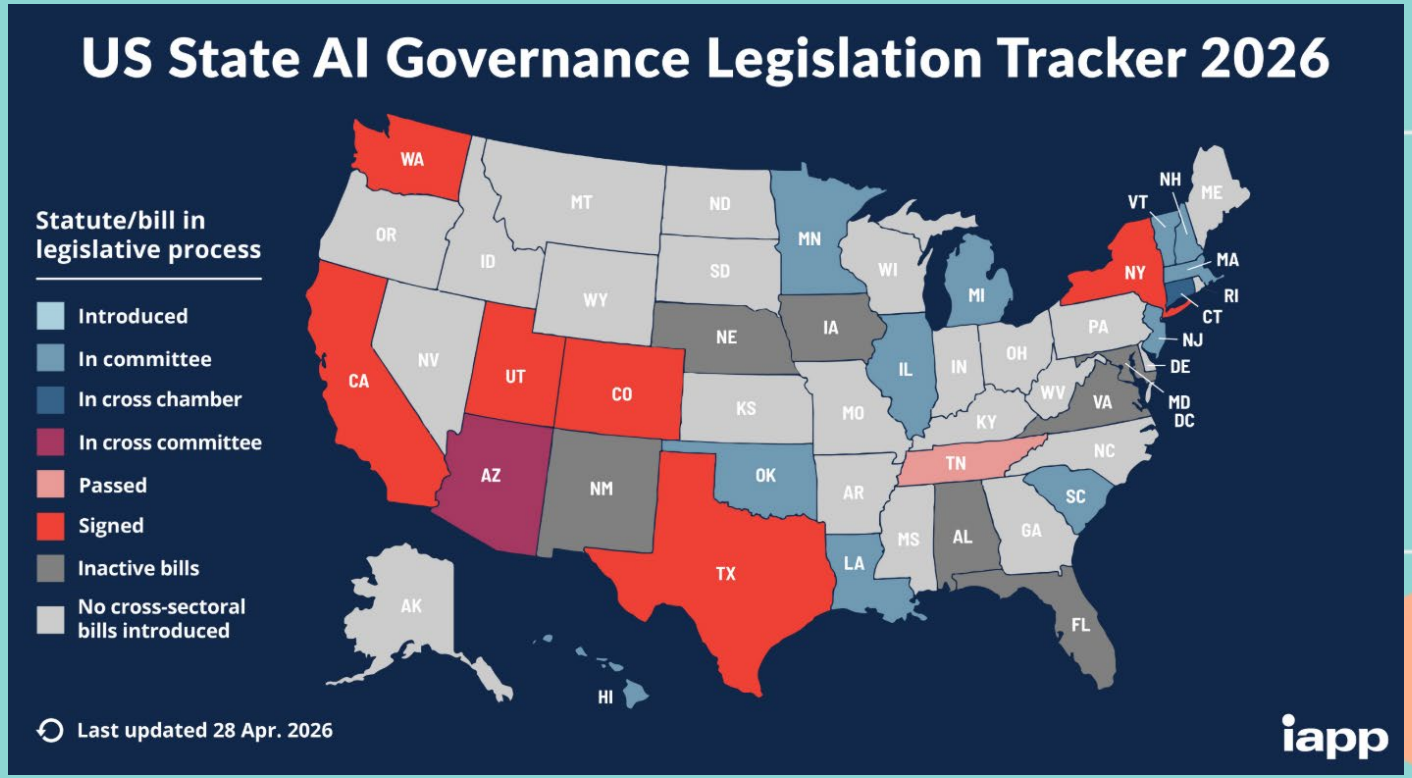
- **“Artificial Intelligence”** - “[A]n AI system [is] an engineered or machine-based system that can, for a given **set of objectives**, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with **varying levels of autonomy**.” (National Institute of Standards and Technology)

- **Generative AI** - artificial intelligence that can generate derived synthetic content, such as text, images, video, and audio, that emulates the structure and characteristics of the artificial intelligence’s training data. (California’s Generative Artificial Intelligence Training Data Transparency)

Some AI-Related Terminology

- **Chatbots** - an artificial intelligence system with a natural language interface that provides adaptive, human-like responses to user inputs; also called AI companions
- **AI Agent** - perform a specific task within defined boundaries; also called a digital assistant
- **Agentic AI** - capable of autonomous action to achieve a specific goal

AI Regulatory Landscape in the US



Used with permission - IAPP, US State AI Governance Legislation Tracker 2026

AI in the Employment Context

- Common Use Cases:
  - Recruitment (e.g., screening applicants, scheduling interviews)
  - Employee management and support (e.g., handling FAQs and inquiries)
  - Performance monitoring (e.g., activity tracking, evaluations)
  - Workplace monitoring (e.g., security)
  - Day-to-day functions (e.g., meeting notetakers)
  - Creating work product (e.g., drafting documents)

Federal AI (De-)Regulation

- January 23, 2025: Executive Order 14179, "Removing Barriers to American Leadership in Artificial Intelligence, rescinded all policies, directives, and regulations established under the Biden administration that could be seen as impediments to AI innovation; emphasizes deregulation to help maintain US AI global dominance.
- December 11, 2025: Executive Order 14365, Ensuring a National Policy Framework for Artificial Intelligence, established a federal policy to "sustain and enhance the United States' global AI dominance through a minimally burdensome national policy framework"
- March 20, 2026: National Policy Framework for AI, covers protecting minors, AI infrastructure, IP protection, "Preventing Censorship," "Enabling Innovation and Ensuring American AI Dominance," "Educating Americans and Developing an A I-Ready Workforce," and "Preempting Cumbersome State AI Laws."
- June 2, 2026: Promoting Advanced Artificial Intelligence Innovation and Security directs government agencies to accelerate AI-enabled cybersecurity initiatives to design a voluntary framework for engagement with developers of frontier AI models before broader release, and to prioritize criminal enforcement against AI-enabled cyberattacks.

Key State AI Laws in Employment Context

We will cover two main types of AI-related laws that apply to employers who are deployers:

1. **Laws about Automated Decision-making Technology in Recruitment and Employment**
   - input is *personal data* and output is an employment-related decision about an individual

2. **Laws Focused on Preventing Bias and Discrimination in Recruitment and Employment**
   - input is not necessarily limited to personal data

SQUIRE PATTON BOGGS

Laws About Automated Decision-making Technology in Recruitment and Employment

CCPA's ADMT Regulations

SQUIRE PATTON BOGGS

Applicability

Automated decision-making technology (ADMT)

&

Used for a significant decision concerning a consumer*

* "consumer" in the CCPA includes California residents who are employees (and their beneficiaries and dependents), independent contractors, and job applicants.

Automated Decision-making Technology

- **Automated Decision-making Technology (ADMT)** - technology that processes *personal data* and uses computation to replace or substantially replace human decisionmaking." (California Consumer Privacy Act (*CPPA*) Regulations)
  - "substantially replace" means "a business uses the technology's output to make a decision without human involvement."
  - "human involvement" means a human reviewer that:
    - knows how to interpret and use the ADMT's output to make a decision;
    - reviews and analyzes the output of the ADMT and other information that is relevant to make or change the decision; and
    - has the authority to make or change the decision based on their analysis.

“Significant Decision”

A decision that results in the provision or denial of:

- Health Care Services
- Financial or Lending Services
- Employment / IC Opportunities or Compensation
- Education Enrollment or Opportunity
- Housing

New ADMT Requirements

SQUIRE PATTON BOGGS

Pre-Use Notice

Right to Opt-Out*

Right to Access

* Subject to exceptions such as human appeal is offered and certain employment-related purposes

Pre-Use Notice

- A business that uses ADMT to make a significant decision concerning a consumer must provide a Pre-Use Notice.
- The Pre-Use Notice must be:
  1. presented *prominently and conspicuously* to the consumer *at or before the point when the business collects* the consumer's personal information that the business plans to process using ADMT*; and
  2. presented in the manner through which the business primarily interacts with the consumer.

* If a business already collected the consumer's personal information for a different purpose and subsequently plans to process it using ADMT to make a significant decision, the business must provide a Pre-Use Notice before processing the consumer's personal information for that purpose.

Pre-Use Notice

- The Pre-Use Notice *must* include the following information:
  1. the specific purpose for which the business plans to use ADMT;
  2. a description of the consumer's right to opt-out of ADMT;
  3. a description of the consumer's right to access ADMT;
  4. a description of how the consumer can submit a request to opt-out of or access ADMT;
  5. a disclaimer that the business is prohibited from retaliating against them for exercising their CCPA rights; and
  6. additional information about how the ADMT makes significant decisions and how the significant decisions would be made if a consumer opts out.

Right to Opt-Out

- A business that uses ADMT to make a significant decision about consumers must provide them with the ability to opt-out of such use of ADMT.
- An opt-out is *not* required (CCPA Reg. 7221(b)):
  1. If the business provides the consumer with a method to appeal the decision to a human reviewer who has the authority to overturn the decision;
  2. For admission, acceptance, or hiring decisions; or
  3. For allocation/assignment of work and compensation decisions.

Right to Access

- When responding to a consumer's request to access ADMT, a business must provide plain language explanations of the following information:
  1. The specific purpose for which the business used ADMT with respect to the consumer;
  2. Information about the logic of the ADMT;
  3. The outcome of the decisionmaking process for the consumer, including how the business used the output of the ADMT to make a significant decision with respect to the consumer; and
  4. That the business is prohibited from retaliating against consumers for exercising their CCPA rights, and instructions for how the consumer can exercise their other CCPA rights.

Right to Access

- A business's methods for consumers to submit requests to access ADMT must be easy to use and must not use dark patterns.
- A business must use reasonable security measures when transmitting information in response to a consumer's access request.
- A business may verify a consumer's request to access ADMT consistent with the verification requirements set forth for the other consumer rights requests (i.e., right to access, right to correct, right to delete).
- If a business denies a consumer's verified request to exercise their right to access ADMT, in whole or in part, because of a conflict with federal or state law, or an exception to the CCPA, the business must inform the requestor and explain the basis for the denial, unless prohibited from doing so by law.

Risk Assessments

- Data Privacy Risk Assessments required for “sale”/”share”, processing of sensitive personal data and high-risk profiling and automated decision-making:
- Using automated processing to infer or extrapolate a consumer’s intelligence, ability, aptitude, performance at work, economic situation, health (including mental health), personal preferences, interests, reliability, predisposition, behavior, location or movements, based on (i) systematic observation of that consumer when they are acting in their capacity as an educational program applicant, job applicant, student, employee or independent contractor of the business; or (ii) the consumer’s presence in a sensitive location; and
- Intends to use personal information to train ADMT for significant decisions.

Risk Assessments

- Risk assessments must include:
  1. the business's **purpose** for processing consumers' personal information
  2. the **categories of personal information** to be processed, including any categories of sensitive personal information and, at a minimum, include the minimum personal information that is necessary to achieve the purpose of processing consumers' personal information
  3. certain **operational elements** of the processing (*as shown in a later slide*)
  4. the **benefits** to the business, the consumer, other stakeholders, and the public from the processing of the personal information, as applicable
  5. the **negative impacts** to consumers' privacy associated with the processing and the sources/causes of these negative impacts
  6. any **safeguards** that the business plans to implement for the processing
  7. **whether it will initiate** the processing subject to the risk assessment
  8. **the individuals** who provided the information for the risk assessment, excluding legal counsel who provided legal advice
  9. **the date** the risk assessment was reviewed and approved, and the names and positions of the individuals who reviewed or approved the risk assessment, except for legal counsel who provided legal advice

Operational Elements

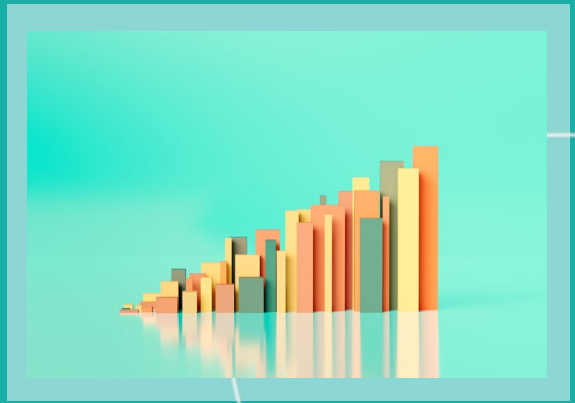
- Methods of collecting, using, disclosing, retaining or otherwise processing
- Sources of the personal information
  - Obligations apply even if business already has the personal information
- Retention details
- Methods of consumer interaction
  - New rights require new processes
- The logic and the output of the ADMT
- Disclosure, notice and consent details
  - Pre-use notice is complicated for a business looking to fast-track technology use
- Details on service providers and third parties that may access or receive personal information

Risk Assessments

- Businesses must *annually* submit certain risk assessment-related information to CalPrivacy, which starts for:
  - Risk assessments from 2026/2027: April 1, 2028
  - Risk assessments after 2027: no later than April 1 the following year
- Businesses, at least once every *3 years*, must review, and update as necessary, its risk assessments to ensure that they remain accurate.
- Businesses must update risk assessments whenever there is a *material change* relating to the processing activity, as soon as feasibly possible, but no later than *45 calendar days* from the date of the material change.
- Businesses must retain its risk assessments, including original and updated versions, for *as long as the processing continues* or for *5 years after the completion of the risk assessment*, whichever is later.

Cybersecurity Audits

- Phased in based on business size:
  - $100M+, April 1, 2028
  - $50M to 100M, April 1, 2029
  - Under $50M, April 1, 2030
- Covers prior calendar year
- Specific audit requirements
- Auditor must be qualified, objective, and independent
- Required data and processing technology inventories
- Requires documentation of audit reports
- Must file compliance certifications with CCPA



Colorado ADMT Law

Automated Decision-Making Technology In Consequential Decisions

- Replaces 2024 CO AI Act
- Enforceable January 1, 2027
- Applies to
  - "**deployer**" which is a legal or natural person doing business in Colorado (6-1-1701(7))
    - Also applies to "developers" (6-1-1701(8))
  - "**consumer**" which includes an employee and a job applicant who is a Colorado resident "whose access to, eligibility for, or opportunity is evaluated in a **consequential decision** by a person doing business in Colorado." (6-1-1701(4)(b))
  - ***"a*utomated decision-making technology" ("ADMT")** means a technology that processes personal data and uses computation to generate output, including predictions, recommendations, classifications, rankings, scores, or other information that is used to make, guide, or assist a decision judgment, or determination concerning an individual. (6-1-1701(1))

Colorado ADMT Law

- **"covered ADMT"** means automated decision-making technology that is used to **materially influence** a consequential decision. (6-1-1701(5))
- **"materially Influence"** means (i) an ADMT output is a non-de minimis factor that is used in making a **consequential decision**; and (ii) an ADMT output affects the outcome of a consequential decision, including by meaningfully altering how a consequential decision is made. (6-1-1701(13))
- **"consequential decision"** means a (i) a decision, determination, or action made about a consumer that relates to the provision of or a consumer's access to, eligibility for, selection for, or compensation for a **covered domain**; or (ii) a decision, determination, or action about a consumer that relates to a differentiated price, cost sharing, compensation, or other material terms in a manner that is reasonably likely to materially limit, delay, effectively deny, or otherwise fundamentally alter the consumer's access, eligibility, or opportunity for a covered domain. (6-1-1701(3))
  - **"covered domain"** includes (a) an **education enrollment or an education opportunity**; (b) employment or an employment opportunity that creates or may create an employer-employee relationship" […] (6-1-1701(6))

Colorado ADMT Law – Deployer Notice

- Deployer must provide notice about Covered ADMT prior to using Covered ADMT to materially influence a consequential decision affecting the consumer
  - prominent public notice that is reasonably accessible at points of consumer interaction
- Deployer must provide, within 30 days after decision with adverse outcome:
  - a plain language description of the consequential decision and the role of the Covered ADMT
    - "adverse outcome" includes a decision that denies, terminates, revokes, or materially reduces or restricts a consumer's access to, eligibility for, selection for, compensation for, or the provision of an opportunity or service
  - instructions for requesting additional information about the Covered ADMT (including "inputs" and other information a developer is required to provide to a deployer)
  - right of meaningful human review and reconsideration "to the extent commercially reasonable" (6-1-1705)
  - rights to access and to correct personal data used in consequential decision

Colorado ADMT Law – Records; Enforcement

- Deployer must retain records "records reasonably necessary to demonstrate compliance" for at least three years after consequential decision
- On or before January 1, 2027, Attorney General must issue regulations, including to "clarify and implement the post-adverse outcome disclosure requirements" and "guidance addressing how the disclosure requirements described in this section interact with federal or state laws that require or govern notices, explanations, or adverse outcome disclosures"
  - Pre-rulemaking request for input: https://coag.gov/app/uploads/2026/06/ADMT-Chatbot-Pre-Rulemaking-Considerations-Document.pdf
- Enforceable by Attorney General - sixty (60) day cure period until January 1, 2030
- Deployer may be held liable in an action alleging unlawful discrimination under state anti-discrimination laws arising from a consequential decision materially influenced by a Covered ADMT. (6-1-1707(17))
  - "Fault shall be allocated among deployers and developers based on their relative fault."
  - Developer is not liable if Covered ADMT is used in a manner that was not "intended, documented, marketed, advertised, configured, or contracted for by the developer."

Connecticut's Artificial Intelligence Responsibility and Transparency (CART) Act

SQUIRE PATTON BOGGS

Connecticut Artificial Intelligence Responsibility and Transparency Act

Four Main Parts:

1. Companion chat bot requirements
2. **Automated Employment-related Decision Technology** (Section 7)
3. Transparency obligations on Covered Providers of AI systems that can generate "synthetic digital content"
4. Whistleblower protections for "covered employee" of large "frontier developer"

CART Act - AEDT

Automated Employment-related Decision Technology (AEDT)

"**AEDT**" is "any technology that processes personal data and uses computation to generate any output, including, but not limited to, any prediction, recommendation, classification, ranking, score or other information, that is a substantial factor used to make or materially influence an employment-related decision."

- "substantial factor" means a factor, a constraint, ranking, score, recommendation or classification, that meaningfully alters the outcome of an employment-related decision.
- "employment-related decision" means a decision, made based on any individual's personal data, to hire, promote, discipline or discharge such individual, to renew such individual's employment, to select such individual for any training or apprenticeship or with respect to such individual's tenure or terms, privileges or conditions of employment

CART Act – Deployer Notice

- "Deployer" that, on or after October 1, 2027, deploys AEDT to "generate any output for the purpose of making, or as a substantial factor in making, an employment-related decision concerning an employee or applicant for employment in Connecticut" must provide pre-use notice disclosing:
  - that AEDT is deployed
  - the purpose and nature of the AEDT and employment-related decision
  - the trade name of the AEDT
  - the categories and sources of personal data that the AEDT will analyze/process and how personal data will be assessed in decision
  - deployer contact information.
- AEDT developer may contract with an AEDT deployer to assume the deployer's duties under sections 9 and 10 (notices). The contract must "clearly set forth" which deployer's duties under sections 9 and 10 are assumed.

SQUIRE PATTON BOGGS

Laws Focused on Preventing Bias and Discrimination in Recruitment and Employment

California CRC Regulations

- The California Civil Rights Council (CRC) (part of what was formerly, the Department of Fair Employment and Housing) implemented regulations amending the existing regulatory framework applicable to the California Fair Employment and Housing Act to clarify how California's anti-discrimination laws apply to the use of AI and automated decision systems (ADS) in employment decision-making.
- An ADS is a "computational process that makes a decision or facilitates human decision making" regarding employment matters.
- The CRC Regulations apply to all employers in California.
  - Employers mean any person or individual engaged in any business or enterprise regularly employing 5 or more individuals, including individuals performing any service under any appointment, contract of hire, or apprenticeship, express or implied, oral or written.

California CRC Regulations

- It is unlawful for an employer or other covered entity to use an ADS or selection criteria (including a qualification standard, employment test, or proxy) that discriminates against an applicant or employee or a class of applicants or employees, subject to any available defense.
- Employers must maintain data on ADS for 4 years.
  - This includes all applications, personnel records, membership records, employment referral records, 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.
- Employers must offer accommodations for AI-based assessments.
  - Assessment that elicit disability-related information before a conditional offer are considered unlawful medical inquiries requiring reasonable accommodations.

New York City Local Law 144

- An employer in New York City (NYC) that uses any automated employment decision tool (*AEDT*) in the hiring processes for any NYC candidate must (among other requirements):
  - undertake an annual bias audit using an independent auditor prior to using an AEDT
  - publish a summary of the bias audit
  - notify the NYC candidate at least 10 business days before AEDT use (An employer can provide notice on its website, in the job posting or by sending to the candidate by mail or email.)
- AEDT means "any computational process, derived from machine learning, statistical modeling, data analytics, or artificial intelligence, that issues simplified output, including a score, classification, or recommendation, that is used to *substantially assist or replace* [*defined in implementing rules*] discretionary decision-making for making employment decisions that impact natural persons"
- Implementing rules enforceable as of July 5, 2023

Illinois Human Rights Act

- **Prohibited Uses**: It is a civil rights violation if an employer:
  - uses AI for Covered AI Uses that have the effect of subjecting employees to discrimination on the basis of protected classes or that use zip code as a proxy for protected classes; and
  - fails to provide notice to an employee that the employer is using AI for the applicable purposes.
- **Covered AI Uses**: recruitment, hiring, promotion, renewal of employment, selection for training or apprenticeship, discharge, discipline, tenure, or the terms, privileges, or conditions of employment

Illinois Department of Human Rights released and then pulled regulations about notice requirements.

New Jersey Rules Pertaining to Disparate Impact Discrimination

- *Published on December 15, 2025* – (N.J.A.C. 13:16)
- The Rules: (i) clarify the application of existing antidiscrimination laws in several contexts, including for any software, system, process (including AI) that aims to automate, aid, or replace human decision-making relevant to employment ("Automated Employment Decision Tools"), and (ii) provide examples of how the use of automated employment decision tools may have a disparate impact on applicants and employees.
- Examples include:
  - The use of automated employment decision tools to make employment decisions, including, but not limited to, decisions related to advertising, recruiting, screening, interviewing, hiring, and compensation, or any other terms, conditions, or privileges of employment, may have a disparate impact on applicants and employees based on their race, national origin, gender, disability, religion, and other protected characteristics.
  - The use of an automated employment decision tool that limits or screens out applicants based on their schedule may have a disparate impact on applicants based on their religion, disability, or medical condition and must include a mechanism for applicants to request a reasonable accommodation.
  - An employer's use of an automated employment decision tool that has not been adequately tested and shown to not adversely affect people in a protected class before its use may have a disparate impact on members of that protected class.

Texas Responsible AI Governance Act (TRAIGA)

Effective January 1, 2026, TRAIGA prohibits an AI system that is developed or deployed:

- to *intentionally* encourage any person to physically harm themselves or others or to engage in criminal activity. (§ 552.052)
- with the *sole intent* of infringing, restricting, or impairing a person's federal Constitutional rights. (§ 552.055(a))
- with the *intent* of unlawful discrimination against a protected class under federal or state law. (§ 552.056(b))
- with the *sole intent* of producing, assisting or aiding in producing, or distributing child pornography or unlawful deepfake videos or images (§ 552.057(1))
- to *intentionally* engage in explicit text-based conversations while impersonating a child under the age of 18 (§ 552.057(2))

Texas Responsible AI Governance Act (TRAIGA)

SQUIRE PATTON BOGGS

TRAIGA's Fines/Penalties

- After receiving a complaint, the Texas AG may issue a civil investigative demand to determine whether a TRAIGA violation has occurred. If a violation is found, a cure notice is required
- If the violation is uncured within 60 days after the cure notice, the Texas AG may bring an enforcement action to enjoin the uncured violations or seek civil penalties:
  - If violation is determined by a court to be curable or a breach of a written "cure" statement: fines of not less than $10,000 and up to $12,000 per violation
  - If violation is determined by a court to be uncurable: fines of $80,000 to $200,000 per violation
  - Continuing violations: fines of up to $40,000 per day the violation continues

- A defendant may not be liable if the defendant discovers a violation via feedback or testing, following state agency guidelines or if the defendant can establish its substantial compliance with the then-current version of NIST AI RMF.

SQUIRE PATTON BOGGS

Other Laws and Issues

AI Scribes

Brewer v. Otter.AI, Inc., No. 5:25-cv-06911 (N.D. Cal. filed Aug. 15, 2025)

August 15, 2025 - complaint relating to meeting recording technology made available by Otter.ai, Inc. (*Otter*)

- Plaintiffs allege that Otter technology
  - Violated the California Invasion of Privacy Act (*CIPA*) by recording and transcribing conversations during Google Meet, Zoom, and Microsoft Teams meetings without the consent of all meeting participants
  - Also violated the California's Comprehensive Computer Data and Fraud Access Act, California common law torts of intrusion upon seclusion and conversion, the California Unfair Competition Law, Electronic Communications Privacy Act of 1986 and the Computer Fraud and Abuse Act

AI Scribes

In re Otter.AI Privacy Litigation (5:25-cv-06911, N.D. California)

December 5, 2025 – consolidated class action

Adds California's statutory prohibition against larceny and the receipt of stolen property, Illinois Wiretapping Law and Washington's Wiretapping Law.

Wiretapping - voice prints are biometric data

- Otter Notetaker violated CIPA "Otter does not obtain prior consent, express or otherwise, of persons who attend meetings where the Otter Notetaker is enabled, prior to Otter recording, accessing, reading, and learning the contents of conversations between Otter accountholders and other meeting participants (or before collecting biometric data)."
- Motion to Dismiss scheduled for July 15, 2026.

[*Other similar lawsuits also have been filed.*]

AI Scribes

Artificial intelligence powered technology that records virtual or in-person meetings and transcribes the recording to written format (*Meeting Recording Technology* or '*AI Scribes*')

Legal Risk Considerations

- Communication Recording Risk
  - State and federal laws prohibit the recording of communications without prior consent.
    - Federal Wiretap Act of 1968, as amended by the Electronic Communications Privacy Act of 1986; California Invasion of Privacy Act
    - Privacy and AI Law Compliance
  - Improper notice and consent required under privacy laws.
- Confidentiality Risk
  - Confidential business information, intellectual property rights, or trade secrets
- Litigation/Government Investigation Risk
  - Waiver of attorney-client privilege because a third party has access to the recordings
- Accuracy Risk
  - If inaccuracies are not detected and corrected in meeting records produced by AI Scribes, they could exacerbate the impact of the legal risks.

Antitrust/Competition Issues

DOJ enforcement involving AI technology that generates output (e.g., compensation recommendations) based on non-public, competitively sensitive information contributed by users of the AI technology.

To date, enforcement focuses on AI technology providers vs. users.

Issues for Users to Consider:

- How many competitors contribute data to/use the AI technology?
  - "give-to-get policy"?
- Is the data real time or aged?
- Is the AI output anonymous in user's hands, i.e., user cannot identify the sources.
- How much does the user rely on the output in making the decision?
  - automatic vs. independent human decision

California AI No Defense Act

- Prohibits a business involved in the development, modification, or use of AI technology from asserting a defense that AI autonomously caused harm to the plaintiff (or AI autonomy as a liability defense)
- Does not impose strict liability simply for using AI
  - Employers using AI must be prepared to defend liability as applicable to their AI use.
- Explicitly preserves other affirmative defenses and evidence relevant to causation, foreseeability, or comparative fault to argue against liability

SQUIRE PATTON BOGGS

Takeaways

Best Practices for HR high risk data processing

Prepare and be proactive:

- Inventory employee and applicant data and technology assets
- Conduct risk assessments and cybersecurity audits
  - Includes auditing AI systems for potential bias or discrimination
- Review and update notices
  - New processes for specific AI/ADMT rights
- Develop, maintain, and update internal policies, procedures, and processes about AI technology deployment
  - Consider all relevant issues – data minimization and retention (e.g., employer's data used as training data?), anti-trust concerns, process for maintaining current notices
  - Revisit cybersecurity (e.g., Anthropic Mythos 5/Fable 5)
  - Consider industry standards (e.g., NIST AI Risk Management Framework)

Best Practices for HR high risk data processing

- Understand Vendors' Technology and Data Use
  - Review or revisit third-party contracts with an AI perspective
  - Update vendor diligence to help identify and address issues before onboarding new AI technology
  - Consider obsolescence risk
- Implement human oversight whenever possible
- Revisit insurance
  - Insurers are moving to exclude losses from certain AI technology use
- Monitor for new and changing AI-specific laws
  - Status of federal-state dynamic
- Conduct regular AI-focused trainings


Questions?

SPB Data Privacy Resources

Powered by SPB

Empower your data strategy with Squire Patton Boggs' comprehensive suite of privacy and cybersecurity tools — designed to help you navigate complex regulations and safeguard digital assets with confidence.

Privacy World Blog

Stay ahead of global data privacy trends with Privacy World Blog— your trusted source for expert analysis, legal updates, and practical guidance in an ever-evolving digital landscape.

Law & Policy Hub

Explore the future of law and technology at the Squire Patton Boggs AI Hub — your gateway to expert insights, legal innovation, and strategic guidance on artificial intelligence.

SQUIRE PATTON BOGGS

Appendix

New York Responsible AI Safety and Education Act

- New York's Responsible AI Safety and Education ("RAISE") Act establishes transparency, safety, and compliance requirements for developers of frontier AI models and mandates safety protocols, independent audits, and disclosure of AI risks to prevent critical harm and ensure responsible AI deployment.
- Applies to "large developers," which means a person that has trained at least one frontier model and has spent over $100,000,000 dollars in compute costs in aggregate in training frontier models.
  - "**Frontier models**" include the following:
    - An artificial intelligence model trained using greater than 10º26 computational operations (e.g., integer or floating-point operations), the compute cost of which exceeds one hundred million dollars; or
    - An artificial intelligence model produced by applying knowledge distillation to a frontier model provided that the compute cost for such model produced by applying knowledge distillation exceeds five million dollars.

Effective January 1, 2027

New York Responsible AI Safety and Education Act

- Key requirements for large developers of frontier models include:
  - Conducting annual safety reviews and independent third-party audits;
  - Publishing information about safety protocols;
  - Reporting safety incidents within 72 hours;
  - Creating a detailed safety and security protocol to prevent such critical harms and engaging in ongoing testing; and
  - Maintaining specific records and reports.

Amendment to the California AI Transparency Act

- Amended to include new obligations for large online platforms, generative AI system-hosting platforms, and capture device manufacturers.
  - A "**large online platform**" is a public-facing social media platform, file-sharing platform, mass messaging platform, or standalone search engine that distributes content to users who did not create, or collaborate in creating, the content, which exceeded 2,000,000 unique monthly users during the preceding 12 months.
  - A "**generative AI hosting platform**" is a website or application that makes available for download the source code or model weights a generative AI system by a resident of the state of California, regardless of whether the terms of that use include compensation.
  - A "**capture device manufacturer**" means a person who produces a capture device for sale in the state. A "capture device" includes any device that can record photographs, audio, or video content, including, but not limited to, video and still photography cameras, mobile phones with built-in cameras or microphones, and voice recorders.
- Extends the deadline for covered providers from the original January 1, 2026 date to **August 2, 2026**, providing an additional seven-month implementation period.

Amendment to the California AI Transparency Act

- Companies must determine whether they qualify as generative AI providers, large online platforms, or capture device manufacturers in order to analyze compliance requirements and effective dates.
- Effective dates:
  - Large online platforms: January 1, 2027
  - Generative AI hosting platforms: January 1, 2027
  - Capture device manufacturers: January 1, 2028
- Violations are enforceable by the California Attorney General and local prosecutors.
- Civil penalties can reach **$5,000 per violation per day** of non-compliance.

California Companion Chatbot Law

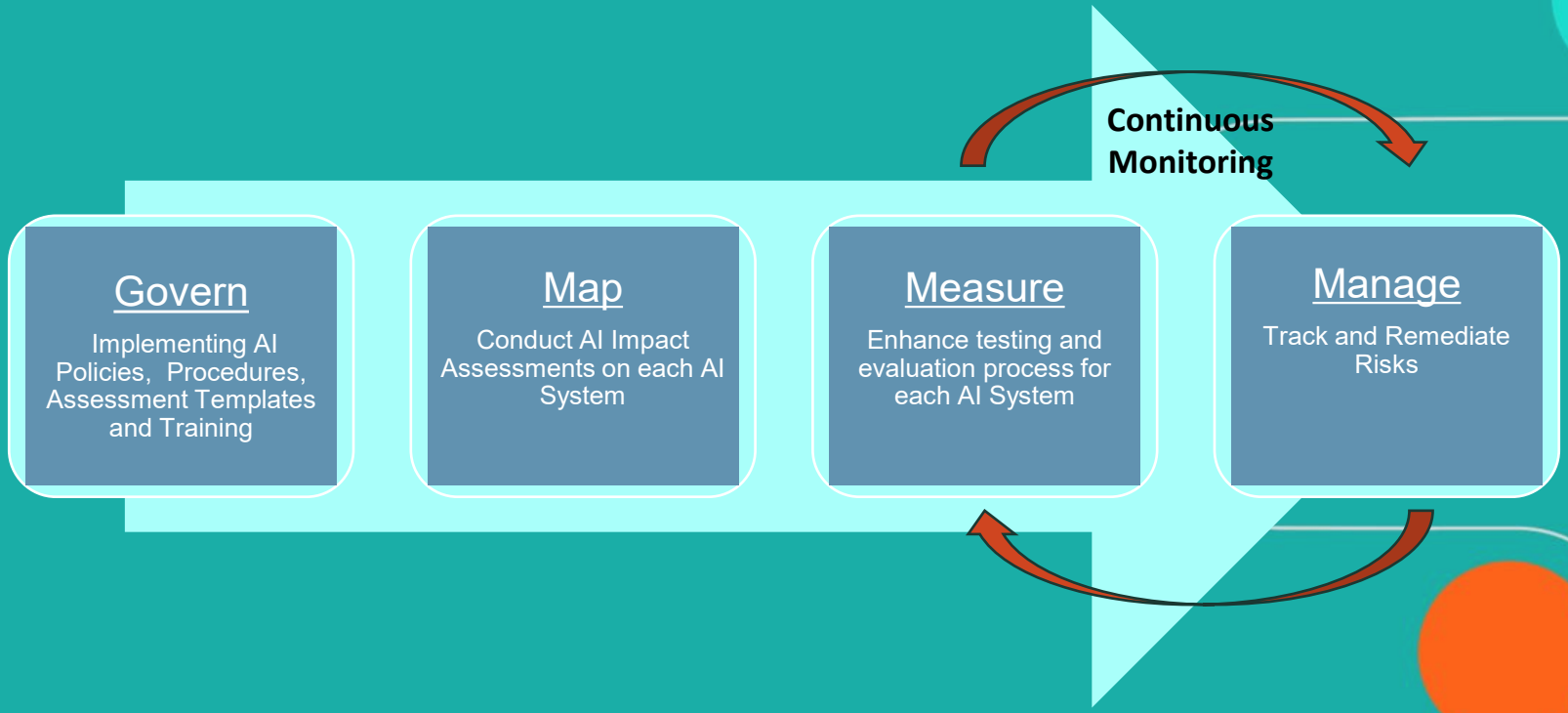
- Establishes specific requirements for operators of "**companion chatbots**"
  - "**Companion chatbots**" mean an AI system with a natural language interface that provides adaptive, human-like responses to user inputs and is capable of meeting a user's social needs, including by exhibiting anthropomorphic features and being able to sustain a relationship across multiple interactions.
  - Excludes:
    - A bot that is used only for customer service, a business' operational purposes, productivity and analysis related to source information, internal research, or technical assistance.
    - A bot that is a feature of a video game and is limited to replies related to the video game that cannot discuss topics related to mental health, self-harm, sexually explicit conduct, or maintain a dialogue on other topics unrelated to the video game.
    - A stand-alone consumer electronic device that functions as a speaker and voice command interface, acts as a voice-activated virtual assistant, and does not sustain a relationship across multiple interactions or generate outputs that are likely to elicit emotional responses in the user.

California Companion Chatbot Law

- Operators of companion chatbots in California must:
  - Maintain a protocol for preventing suicidal ideation, suicide, or self-harm content to all users and publish protocol details on their websites;
  - Make certain notifications and/or disclosures to minors; and
  - Report annually to the California Office of Suicide Prevention.
- Creates a private right of action, allowing individuals harmed by a violation to bring a civil action and exposes companies to potential lawsuits and significant penalties (damages of at least $1,000 per violation, plus attorney's fees).

Effective January 1, 2026.

Implementation Strategy for Aligning to NIST



Implementing an AI Risk Management Program

SQUIRE PATTON BOGGS

Create AI System Inventory

Develop inventory of AI systems which documents the AI System Name, AI System Owner, System Description, other descriptive information and if the AI System is consider High Risk pursuant to in scope AI regulations.

Conduct NIST AI RMF or ISO Assessment

Conduct assessment using NIST AI RMF or ISO 42001 standards. Utilize assessment process to assess current state, gain alignment with organization stakeholders and determine future priorities.

Develop Roadmap

Using the output from the assessment, develop implementation roadmap to detail how toolkits will be operationalized. For example, certain aspects of client's existing program will be enhanced whereas in other cases the toolkit will be net new.

Operationalize Toolkits and Remediate Gaps

Operationalize toolkits or enhance existing artifacts to meet NIST/ISO standards:

1. AI Risk Management Policy
2. Inventory of AI Systems *(complete)*
3. AI Impact Assessment Template
4. AI System Performance and Monitoring Template
5. AI System Risk Register
6. AI Incident Response Plan
7. Third Party Risk Management
8. AI Risk Management Training
9. Channels to receive AI updates