

California and Beyond: HR Data Risk Issues for Employers

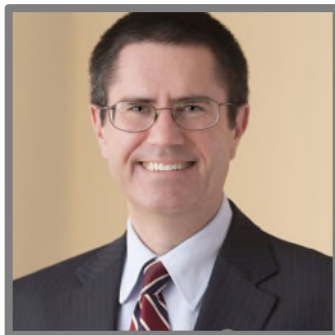
February 26, 2026
1:00 PM ET





Alan L. Friel

Partner
Data Privacy, Cybersecurity &
Digital Assets
(Los Angeles)
alan.friel@squirepb.com



Michael W. Kelly

Partner
Labor & Employment
(San Francisco)
michael.kelly@squirepb.com



Sammuel Kim

Associate
Data Privacy, Cybersecurity &
Digital Assets
(New York)
sammuel.kim@squirepb.com

- New *privacy risk assessments*, cybersecurity and data subject notice and choice obligations for employers under the CCPA
- Other *risk and bias assessment* obligations applicable to AI and ADM for US employers
- *Other AI and ADM compliance* obligations for US employers
- *Trade secret and antitrust issues* with platform use
- Special consideration for *biometrics and other sensitive personal data*
- *Best practices* for HR high risk data processing

Overview

- AI usage in HR is becoming common for:
 - Recruitment (e.g., screening applicants, onboarding process)
 - Employee management and support (e.g., payroll, benefits, chatbots for FAQs and inquiries)
 - Performance monitoring (e.g., calculating metrics, activity tracking, evaluations)
 - Workplace monitoring (e.g., surveillance, security, tracking)
 - Day-to-day functions (e.g., spelling/grammar check, email management, meeting notes)
 - Creating work product (e.g., drafting documents)
- The most common form of AI used in the HR context is generative AI.
 - Generative AI typically refers to algorithms that create new content, including text, images, code, videos, and audio, by learning patterns from datasets.
 - In order for the AI to work, AI needs training data to improve logic and create outputs.
 - Inputs may be private and restricted or used cross-platform.

- In order to keep up with the increased usage of AI in the workplace, state legislators are moving quickly to enact laws and regulations to govern the use of AI in the HR context.
 - The feds are taking a more retained approach to foster innovation.
- As a result, employers face multiple legal and regulatory risks by employing AI in the workplace, including:
 - Potential class action lawsuits
 - Data privacy and security claims
 - Employment claims
 - Fines and enforcement by regulators

- Trump 2.0 Executive Order: 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 (January 23, 2025)
- White House issued a “Request For Information on the Development of an Artificial Intelligence (AI) Action Plan” (February 6, 2025)
 - Sought public input on priority policy areas “to ensure that unnecessarily burdensome requirements do not hamper private sector AI innovation”
 - Comment period closed March 15, 2025
- The Federal Office of Management and Budget issued two revised policies on Federal Agency Use and Federal Procurement of AI (April 3, 2025)
 - OMB Memorandum M-25-21 “Accelerating Federal Use of AI through Innovation, Governance, and Public Trust”; “Policies introduce a single ‘high-impact AI’ category to track AI use cases that require heightened due diligence because of potential impacts on the rights or safety of the American people”
 - OMB Memorandum M-25-22 “Driving Efficient Acquisition of Artificial Intelligence in Government”; “Agencies will use performance-based techniques to best harness the rapidly developing AI marketplace and create an online shared repository of resources and tools to assist with AI procurement”

- Proposed preemptive moratorium on state AI laws introduced in Senate
 - The moratorium was pitched as necessary to allow US AI developers to innovate and help ensure US leadership in AI
 - Senate first considered a 10-year ban, then a 5-year ban and ultimately voted 99-1 *against* the moratorium (July 1, 2025)
- White House announced \$90 billion in “groundbreaking AI and energy investments in Pennsylvania” (July 15, 2025)
 - Goal of investment is to accelerate the development of artificial intelligence infrastructure in Pennsylvania; similar AI infrastructure announcements expected in near future
- AI Summit and AI Action plan
 - Three Executive Orders expected (July 22, 2025)
 - “Winning the AI Race” (summit in Washington DC) (July 23, 2025)
 - AI Action plan is expected to focus on anti regulation/pro growth

- On December 11, 2025, President Trump signed Executive Order 14365, “*Ensuring a National Policy Framework for Artificial Intelligence*,” which among other things, establishes a federal policy to “sustain and enhance the United States’ global AI dominance through a minimally burdensome national policy framework for AI”
 - The EO, which builds out President Trump’s July 2025 AI Action Plan, specifically aims to address the increasing number of state AI-related laws and regulations by establishing a series of steps to challenge or preempt state laws that conflict with the Trump administration’s goals
- Despite President Trump’s EO, states continue to file new bills proposing AI-related laws and regulations in 2026
 - Many bills from 2025 are also being carried over and have seen movement this year

New Obligations for Employers under the CCPA

- California's CalPrivacy finalized a sweeping rulemaking package implementing regulations regarding automated decision-making technology (ADMT), risk assessments, and cybersecurity audits
 - On July 24, 2025, the Board approved the draft regulations
 - On September 25, 2025, the Board advanced the CA OAL-approved updates
- Finalized implementation schedule:
 - ADMT requirements – January 1, 2027
 - Security Audits – Depends on business's gross revenue
 - Data Processing Risk Assessments:
 - Activities initiated on or after January 1, 2026 are subject to risk assessments
 - Documentation for activities before that effective date, but continuing after, not required until December 31, 2027, and filing due on April 21, 2028
 - Other amendments – effective as of January 1, 2026

Applicability

Automated decision-making
technology processing PI



Used for a significant decision
concerning a **consumer***

* **Consumer** means a natural person who is a California resident, and may include employees (their beneficiaries and dependents), independent contractors, and job applicants.

- “any technology that processes personal information and uses computation to replace human decisionmaking or substantially replace human decisionmaking”
 - “Substantially replace” means “a business uses the technology’s output to make a decision without human involvement”
 - “Human involvement” is defined as requiring the human reviewer to:
 - Know how to interpret and use the technology’s output to make a decision;
 - Review and analyze the output of the technology and other information that is relevant to make or change the decision; and
 - Have 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

Pre-Use Notice

Right to Opt-Out*

Right to Access

- *Subject to exceptions such as permitted uses or if human appeal is offered
And many HR purposes*

- 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:
 - 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
 - presented in the manner in which the business primarily interacts with the consumer.

* If a business has 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.

- The Pre-Use Notice *must* include the following information:
 - the specific purpose for which the business plans to use ADMT;
 - a description of the consumer's right to opt-out of ADMT;
 - a description of the consumer's right to access ADMT;
 - a description of how the consumer can submit a request to opt-out of or access ADMT;
 - a disclaimer that the business is prohibited from retaliating against them for exercising their CCPA rights; and
 - additional information about how the ADMT works to make significant decisions, and how the significant decisions would be made if a consumer opts 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:
 - 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;
 - **For admission, acceptance, or hiring decisions; or**
 - **For allocation/assignment of work and compensation decisions.**

- A business that *uses ADMT to make a significant decision* must provide a consumer with information about this use when responding to a consumer's request to access ADMT.
- When responding to a consumer's request to access ADMT, a business *must* provide plain language explanations of the following information:
 - The specific purpose for which the business used ADMT with respect to the consumer;
 - Information about the logic of the ADMT;
 - 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
 - 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.

- 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.

- Most of the state privacy laws require that Data Privacy Impact Assessments (DPIAs) of “high risk” data practices are documented and available for inspection
 - Only Iowa and Utah do not contain this requirement
 - MN and CA (as part of 7123(b)(2)(E) auditing) require data inventories

- California adds to typical CPL assessment triggers of sale/share/target, **processing of sensitive personal data and high-risk profiling / automated decision making**:
 - (1) 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 (1) 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 (2) the consumer’s presence in a sensitive location; and
 - (2) Intends to use personal information to train ADMT for significant decisions.

- Risk assessments must include:
 - the business's **purpose** for processing consumers' personal information
 - 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
 - certain **operational elements** of the processing (*as shown in a later slide*)
 - the **benefits** to the business, the consumer, other stakeholders, and the public from the processing of the personal information, as applicable
 - the **negative impacts** to consumers' privacy associated with the processing and the sources/causes of these negative impacts
 - any **safeguards** that the business plans to implement for the processing
 - **whether it will initiate** the processing subject to the risk assessment
 - **the individuals** who provided the information for the risk assessment, excluding legal counsel who provided legal advice
 - **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

- Methods of collecting, using, disclosing, retaining or otherwise processing PI, and the sources of the PI
- Retention details
- Methods of data subject interaction
- Approximate number of data subjects
- Disclosure, notice and consent details
- Details on service providers and third parties that may access or receive PI
- For ADMT:
 - the logic; and
 - the output

- 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.

- 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
- Very 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

- Every business whose processing of consumers' personal information presents *significant risk to consumers' security* must complete a cybersecurity audit.
- A business's processing of consumers' personal information presents *significant risk to consumers' security* if any of the following is true:
 - The business derives 50% or more of its annual revenues from selling or sharing consumers' personal information; or
 - As of January 1 of the calendar year, the business had annual gross revenues in excess of \$25,000,000* in the preceding calendar year; and
 - Processed the personal information of 250,000 or more consumers or households in the preceding calendar year; or
 - Processed the sensitive personal information of 50,000 or more consumers in the preceding calendar year.

*Adjusted for inflation, which is currently \$26,625,000.

- Cybersecurity audits must assess:

- The business's establishment, implementation, and maintenance of its cybersecurity program, including the related written documentation thereof (e.g., policies and procedures), that is appropriate to the business's size and complexity and the nature and scope of its processing activities, taking into account the state of the art and cost of implementing the components of a cybersecurity program
- How the business implements and enforces compliance with its cybersecurity program
- Each of the following components of a cybersecurity program (as applicable):

- Authentication (including MFA)
- Encryption of PI, at rest and in transit
- Account management and access controls
- Inventory and management of personal information and the business's information system
- Secure configuration of hardware and software
- Antivirus and antimalware protections
- Segmentation of information systems
- Limitation and control of ports, services, and protocols
- Cybersecurity awareness
- Cybersecurity education and training
- Secure development and coding best practices
- Oversight of service providers, contractors, and third parties
- Retention schedules and proper disposal of personal information no longer required to be retained
- How the business manages its responses to security incidents
- Business-continuity and disaster-recovery plans

- Each calendar year that a business is required to complete a cybersecurity audit, it must submit to CalPrivacy a written certification that the business completed the cybersecurity audit as required no later than April 1 of the following year
- The certification *must* include:
 - The business's name and point of contact for the business, including the contact's name, phone number, and email address
 - A statement that the business has completed the cybersecurity audit
 - The time period covered by the cybersecurity audit, by month and year
 - An electronically signed attestation to the following statement:
 - “I attest that I meet the requirements of California Code of Regulations, Title 11, section 7124, subsection (c), to submit this certification. Under penalty of perjury under the laws of the state of California, I hereby declare that the information contained within and submitted with this certification is true and correct and that the business has not made any attempt to influence the auditor's decisions or assessments regarding the cybersecurity audit.”
 - The name and business title of the person submitting the certification, and the date of the certification

Other risk and bias assessment obligations applicable to AI and ADM for US employers

- 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.

- 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 (previously 2 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.

- 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

- 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 to use zip codes as a proxy for protected classes; and
 - fails to provide notice to an employee that the employer is using artificial intelligence 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 is expected to adopt rules related to notice requirements.

- 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.
- Such 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.

Other AI and ADM compliance obligations for US employers

“Concerning Consumer Protections In Interactions With Artificial Intelligence Systems” (Colorado AI Act)

- Enacted May 17, 2024; *operative June 30, 2026*
- Applies to a legal and natural person operating in Colorado and that/who is a “**developer**” and/or “**deployer**” (user) of any “High-Risk Artificial Intelligence System” (**HAIS**) or “Artificial Intelligence System.”
- HAIS means:
 - any **Artificial Intelligence System** that
 - makes or is a **Substantial Factor** in making
 - a **Consequential Decision**



- **Duty of Care**: Exercise a duty of care to protect consumers from Algorithmic Discrimination.
- **Risk Management Policy and Program**: Implement a risk management policy and program for HAIS use that includes specific “principles, processes and personnel” used to identify, document and mitigate known or reasonably foreseeable risks of **Algorithmic Discrimination** over the HAIS’ lifecycle.
- **Impact Assessment**: Complete an impact assessment for deployed HAIS at least annually and within 90 days after any intentional and substantial modification to the HAIS.
 - Specified content requirements include a description of inputs and outputs; metrics used to evaluate performance and limitations; a description of transparency measures; and a plan for post-deployment monitoring.

Four Main Transparency Obligations

- i. **Pre-Deployment Notice for HAIS**: Prior to the deployment of a HAIS that makes or is a Substantial Factor in making a Consequential Decision, the Deployer must **notify affected Consumers** about the HAIS, including its purpose and the nature of the Consequential Decision; the contact information for the Deployer; how to access the Deployer's statement about its HAIS use and risk management; and how to access information about the Consumer's right to opt out of the processing of personal data concerning the Consumer for purposes of profiling in furtherance of decisions that produce legal or similarly significant effects concerning the Consumer.
- ii. **Adverse Consequential Decision Notice for HAIS**: The Deployer must provide a **direct notice to a Consumer who was the subject of an adverse Consequential Decision**, including the reasons for the adverse Consequential Decision and type(s) of data processed in making the adverse Consequential Decision and the sources of that data, the Consumer's right to correct incorrect personal data used in the HAIS' Consequential Decision and the Consumer's right of appeal for the Consequential Decision.

- iii. **Website Statement about HAIS**: The Deployer must make available a clear and readily available website statement that is periodically updated about the Deployer's currently deployed HAIS, how the Deployer manages known or reasonably foreseeable risks of Algorithmic Discrimination and the nature, source, and extent of the information collected, and used by the Deployer "in detail."

- iv. **Generative AI Notice**: The Deployer must provide notice to Consumers about the Deployer's Artificial Intelligence System (i.e., broader than HAIS) with which the Consumer interacts unless the interaction with the Artificial Intelligence System "would be obvious to a reasonable person."

- Prohibits businesses involved in the development, modification, or usage of AI from asserting a defense that AI autonomously caused harm to the plaintiff (or AI autonomy as a liability defense)
 - The law was passed to ensure that deployers of AI remain accountable for resulting damages.
- Does not impose strict liability simply for using AI
 - This means 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

- In 2020, Illinois enacted the Artificial Intelligence Video Interview Act ([820 ILCS 42](#)) to govern the use of **AI to assess video interviewees** for jobs in Illinois.
- Employers recruiting in Illinois should take special care to:
 - obtain consent from applicants before using AI, after explaining how the AI works and its evaluation standards; and
 - ensure proper control of video recordings and deletion upon request.
- Requires employers who rely solely on AI to analyze video interviews to determine whether an applicant will be selected for an in-person interview, to collect and report to the Department of Commerce and Economic Opportunity annually on the demographic data of the applicants.

- In 2020, Maryland passed its AI-employment law, H.B. 1202.
- H.B. 1202 prohibits employers from using facial recognition technology during an interview for employment to create a facial template without consent.
- Consent requires a signed waiver that states:
 - the applicant's name;
 - the date of the interview;
 - that the applicant consents to the use of facial recognition; and
 - whether the applicant read the consent waiver.

Utah Artificial Intelligence Policy Act – *operative May 1, 2024*

A business or individual that “uses, prompts, or otherwise causes [GenAI] to interact with a person” to “clearly and conspicuously disclose” that the person is interacting with GenAI (not a human) “if asked or prompted by the person”; persons in “regulated occupations” (generally, need a state license or certification) must “prominently” disclose that a consumer is interacting with generative AI in the provision of the regulated services.

Maine’s “Act to Ensure Transparency in Consumer Transactions Involving Artificial Intelligence” – *operative September 24, 2025*

“A person may not use an artificial intelligence chatbot or any other computer technology to engage in trade and commerce with a consumer in a manner that may mislead or deceive a reasonable consumer into believing that the consumer is engaging with a human being unless the consumer is notified in a clear and conspicuous manner that the consumer is not engaging with a human being.”

Special consideration for biometrics and other sensitive personal data

Recent amendments to the CPA impose new biometrics-related obligations.

- The biometric amendments to the Colorado Privacy Act obligates a broader range of organizations than the rest of the Colorado Privacy Act.

A controller that processes any amount of biometric identifiers or biometric data must comply with the Colorado Privacy Act's requirements for biometric identifier or biometric data, which includes the same "duties" as for other personal data, i.e., transparency, purpose specification, data minimization, avoid secondary use, care, avoid unlawful discrimination and regarding sensitive data (including prior consent).

- Employees are in scope of the biometric amendments.
 - *If a controller collects biometric identifiers from an employee, the controller must obtain **consent** to collect and process the biometric identifiers. A controller may not condition employment on an employee or prospective employees' consent, except to permit access to secure physical locations, electronic hardware and software applications; record the employees work day; improve or monitor workplace safety or security or ensure the safety or security of employees; or improve or monitor public safety or security during emergencies or crisis.*
- This means that employers must comply with the new obligations set forth by the biometric amendments.
 - **Notice Requirement:** must provide employees with a notice in a clear, reasonably accessible, and understandable manner prior to collecting biometric identifiers from them.
 - **Written Policy Requirement:** must develop a written policy that establishes a retention schedule for, a protocol for responding to a data security incident that compromise the security of and governs deletion of employees' biometric identifiers and/or biometric data.

Trade secret and antitrust issues with platform use

- Sharing competitively sensitive information—including wage information—with competitors may violate antitrust laws
 - Providing competitively sensitive information through an algorithm or through a third party's tool or product may be unlawful.
 - *For example, the DOJ obtained a court-ordered settlement with a group of poultry processing companies and a data consulting company to resolve allegations that they (i) directly exchanged competitively sensitive information about current and future wages and benefits for plant workers; and (ii) did so through a third-party firm that facilitated the exchange of competitively sensitive compensation information.*
 - Information exchanges facilitated by or through a third party (including through an algorithm or other software) that are used to generate wage or other benefit recommendations can be unlawful even if the exchange does not require businesses to strictly adhere to those recommendations.

Best Practices for HR high risk data processing

Prepare and be proactive:

- Engage legal counsel to conduct an overall legal assessment
 - Legal counsel may assist in better understanding specific obligations (e.g., which laws apply) and analyzing/weighing the risks of the use of AI
- Inventory and protect HR data and assets
- Conduct data processing risk assessments and cybersecurity audits
 - This includes auditing AI systems for potential bias or discrimination
- Develop, maintain, and update internal policies, procedures, and processes, as needed
 - Comply with industry standards (e.g., NIST AI Risk Management Framework)
- Review or revisit third-party contracts with an AI perspective
- Implement human oversight where possible
- Conduct regular AI-focused trainings

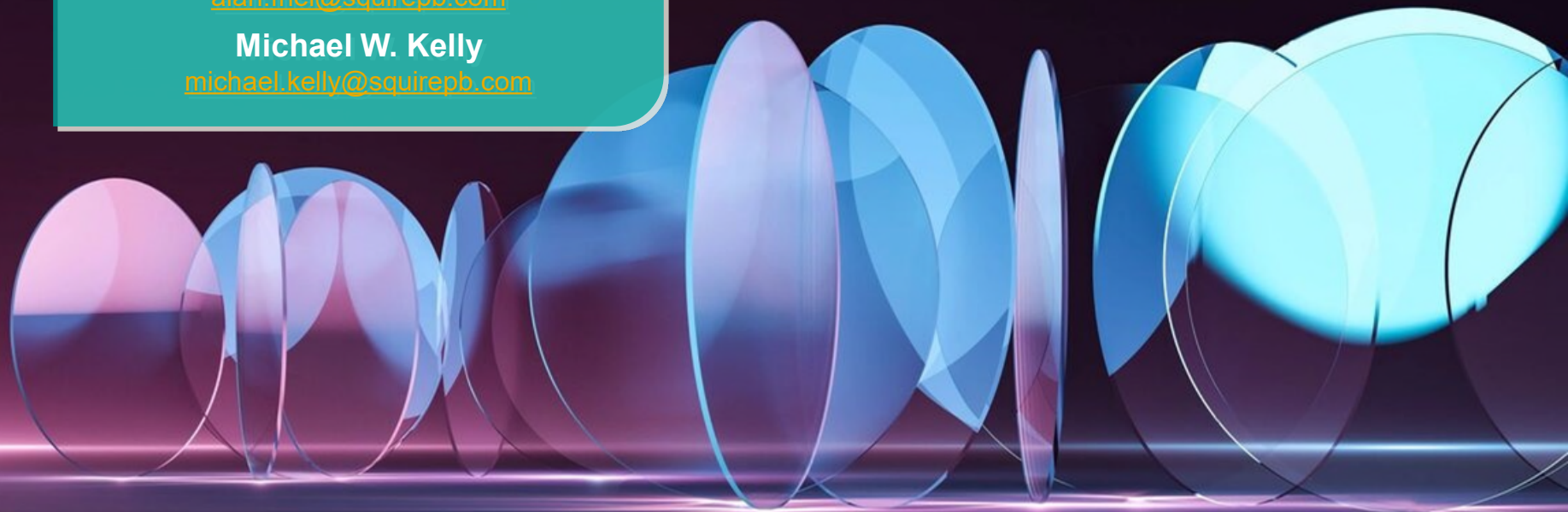
Questions?

Alan L. Friel

alan.friel@squirepb.com

Michael W. Kelly

michael.kelly@squirepb.com



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.

- 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.

- 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.

- 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.

- 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.

1. **Duty of Care**: Exercise a duty of care to avoid Algorithmic Discrimination arising from “intended and contracted uses.”
2. **Documentation for Deployers**: Make certain documentation available for Deployers, including purpose and intended benefits and uses of the HAIS; known and reasonably foreseeable limitations, including risks of Algorithmic Discrimination; training data set use and governance; and how the Deployer should use / not use the HAIS and when human monitoring is advisable.
3. **Impact Assessment Information**: Make available documentation sufficient for a Deployer of the HAIS to conduct an impact assessment.
4. **Website Statement**: Post a public website statement about the types of HAIS that the Developer has developed and how the Developer manages known or reasonably foreseeable risks of Algorithmic Discrimination during development.
5. **Attorney General Notification and Information Requests**: Notify the Attorney General and known Deployers within 90 days after a discovery of, or credible report about an HAIS’ Algorithmic Discrimination risks arising from intended uses and respond to other information requests from the Attorney General.

Texas Responsible AI Governance Act (TRAIGA)

- Effective January 1, 2026, TRAIGA applies to the development or deployment of an AI system by private-sector entities that conduct business in Texas, produce a product or service used by Texas consumers, or develop or deploy an AI system in Texas.
- A defendant is not liable for an AI system because a third party uses an AI system for a prohibited purpose under TRAIGA. (§ A552.105(e))
 - The issue is the developer's or deployer's intent in developing and distributing an AI system, not how the AI system is used.
 - Rebuttable presumption that a business used "reasonable care." (§ A552.105(c))
- No private right of action.
- The Texas Attorney General (AG) must create an online mechanism to receive complaints.

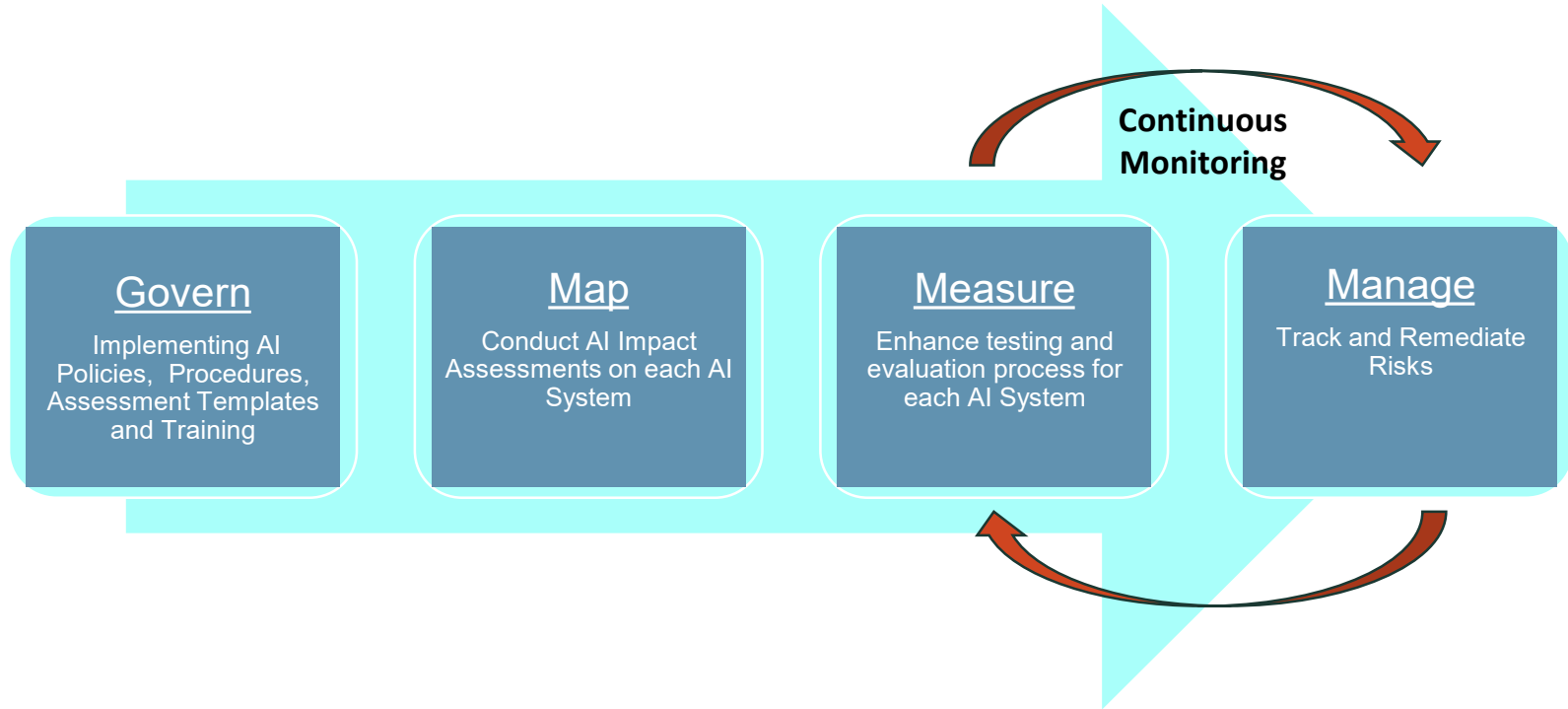
TRAIGA prohibits an AI system that is developed or deployed:

- 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))

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.

Implementation Strategy for Aligning to NIST



Implementing an AI Risk Management Program

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