HUNTON
ANDREWS KURTH

FALL 2024

AI and Emerging Technologies

LABOR AND EMPLOYMENT

Employee Monitoring: Increased Use Draws Increased Scrutiny from Consumer Financial Protection Bureau

On October 24, 2024, the Consumer Financial Protection Bureau (CFPB) issued a policy statement (known as a Circular) to explain the link between the Fair Credit Reporting Act (FCRA) and employers' growing use of artificial intelligence (AI) to evaluate, rank, and score applicants and employees. Employers should take note that the FCRA does not only apply to criminal history or credit reports. As the use of advanced data analysis and AI rise, employers should ensure that they are not running afoul of the FCRA's requirements.

Consumer Reporting Tools

The CFPB notes that vendors now offer a range of products and services to employers, including those that record workers' activities, personal habits, tendencies, attributes, and, in some cases, biometric information. Some employers use this information to, e.g., track worker productivity and evaluate performance.

Vendors also offer similar products and services that provide insights into prospective employees. As an example, the CFPB highlighted a phone app that monitors a transportation worker's driving activity and provides driving scores to companies for employment purposes.

The CFPB's Circular makes clear to employers that some of these vendors may be considered, under the FCRA, as consumer reporting agencies, and the products and services they provide may fall under the definition of a "consumer report," triggering a host of accuracy, notice, and transparency requirements.

FCRA's Reach

Under the FCRA, a consumer reporting agency is a company that "regularly assembles or evaluates consumer information" into a consumer report and sells that information to third parties.

In turn, a consumer report is "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for" certain purposes, including "employment purposes."

If employers seek to use information in a consumer report for an adverse employment action, there are various disclosure and notice requirements that must be complied with prior to taking action.

What Does the Circular Mean for Employers?

Employers should assess the current technological tools they are using, including AI, to determine whether those tools may constitute consumer reports, triggering the need to comply with the FCRA. The CFPB notes that "[a] company that employers use to help make employment decisions could meet this standard in a number of ways." For example, in the applicant realm, consumer reporting agencies may offer data (e.g., disciplinary or performance trends) about applicants gathered from other employers. If employers are using this information to make employment decisions, that data may fall within the ambit of the FCRA.

Employers or vendors with questions about the FCRA, and the CFPB's circular, should consult with their labor and employment attorneys and stay abreast of developments in the law.

Kevin J. White
Partner, Washington, DC and Houston

Daniel J. Butler
Associate, Miami

Illinois Enacts New Law Regulating Employer Use of Artificial Intelligence

On August 9, 2024, Illinois Governor J.B. Pritzker signed H.B. 3773 into law, requiring all Illinois employers to notify employees and applicants when they use artificial intelligence (AI) to make employment decisions. The law broadly defines AI to mean:

> 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." AI includes generative artificial intelligence.
>
> *See* 775 ILCS 5/2-101(M).

Additionally, the law prohibits employers from using AI for recruitment, hiring, promotion, renewal of employment, selection for training or apprenticeship, discharge, discipline, tenure or other terms, privileges, or conditions of employment in a way that is discriminatory based on protected classes. The new law also prohibits employers from using ZIP codes as a proxy for protected classes.

HB 3773 directs the Illinois Department of Human Rights to adopt any rules necessary for the implementation and enforcement of the law, including rules on the circumstances and conditions that require notice, the time period for providing notice, and the means for providing notice.

When Does the Law Go into Effect?

The legislation will go into effect on January 1, 2026.

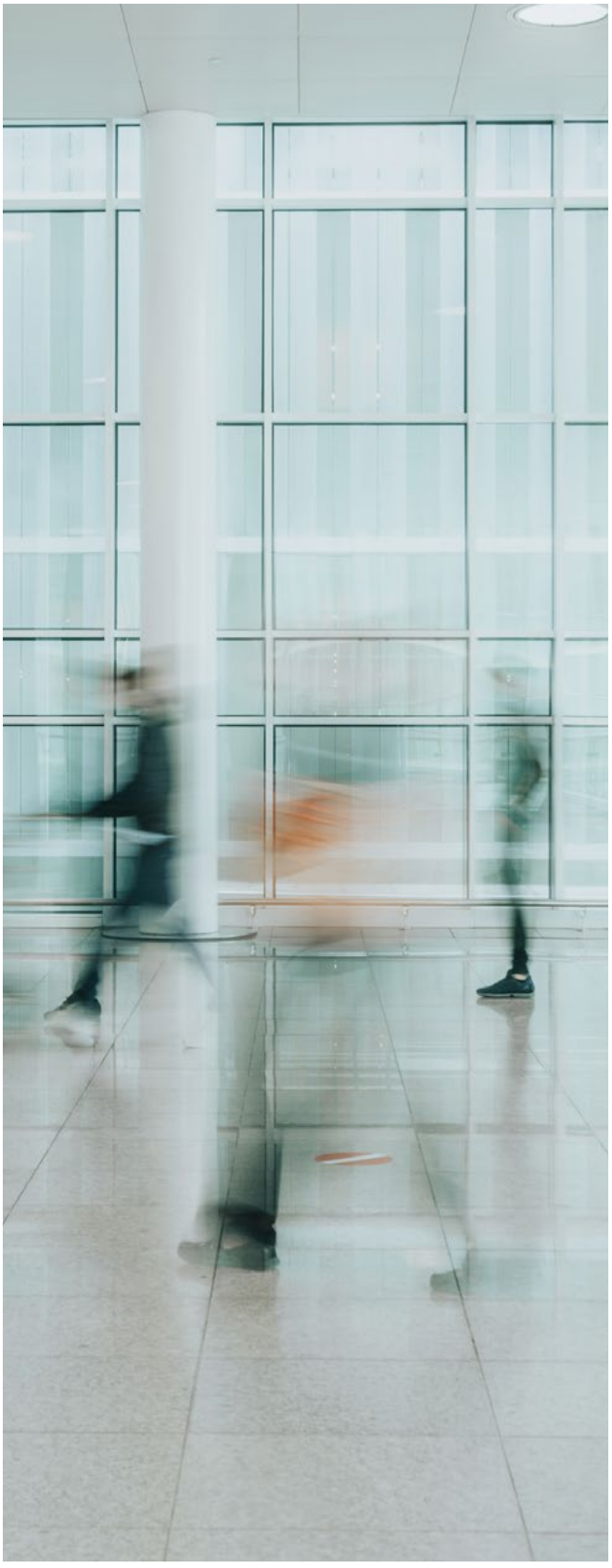
Who Is Covered by the Law?

Any person or entity that employs at least one employee in Illinois.

How Did We Get Here?

In recent years the use of AI in employment has grown tremendously. Employers have used AI for automated candidate sourcing, resume screening, applicant testing, and performance management. As employer use of AI has increased, so has federal and state legislative efforts to regulate its use.

Even though there is currently no federal law regulating employer use of AI, federal agencies have issued instructive guidance. For example, on May 12, 2022, the Equal Employment Opportunity Commission (EEOC) issued guidance, "The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees." The guidance explains



how the use of AI may violate the Americans with Disabilities Act (ADA) and provides tips on how to avoid doing so. In April 2024, the Department of Labor (DOL) issued DOL Field Assistance Bulletin No. 2024-1, "Artificial Intelligence and Automated Systems in the Workplace Under the FLSA and Other Federal Labor Standards" (April 29, 2024) to address potential issues under the Fair Labor Standards Act (FLSA) when employers use AI to perform tasks such as setting work schedules and tracking work hours. Also, on May 16, 2024, the Department of Labor (DOL) developed "Artificial Intelligence and Worker Well-being: Principles for Developers and Employers" as directed by President Biden's October 30, 2023 Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.

Various states have also enacted laws governing employer use of AI In May 2024, Colorado became the first state to mandate disclosures to employees and applicants when employers use AI in employment decisions. Also, Maryland regulates the use of facial recognition services to create a facial template during an applicant's interview without a signed waiver by the applicant.

HB3773 is not Illinois' first attempt to regulate the use of AI in employment decisions. Effective January 1, 2020, Illinois enacted the Artificial Intelligence Video Interview Act (AIVI Act) which requires employers to provide applicants with advance notice that they may use AI, inform applicants how AI works, obtain applicant's consent to be evaluated by AI, and delete the video within 30 days of the applicant's request. Under the AIVI Act, employers are prohibited from sharing applicant video except with people whose expertise is necessary to evaluate the applicant. As of January 1, 2022, employers who use AI analysis of video interviews as the sole method of determining whether an applicant is selected for an in-person interview must collect and report the race and ethnicity of applicants.

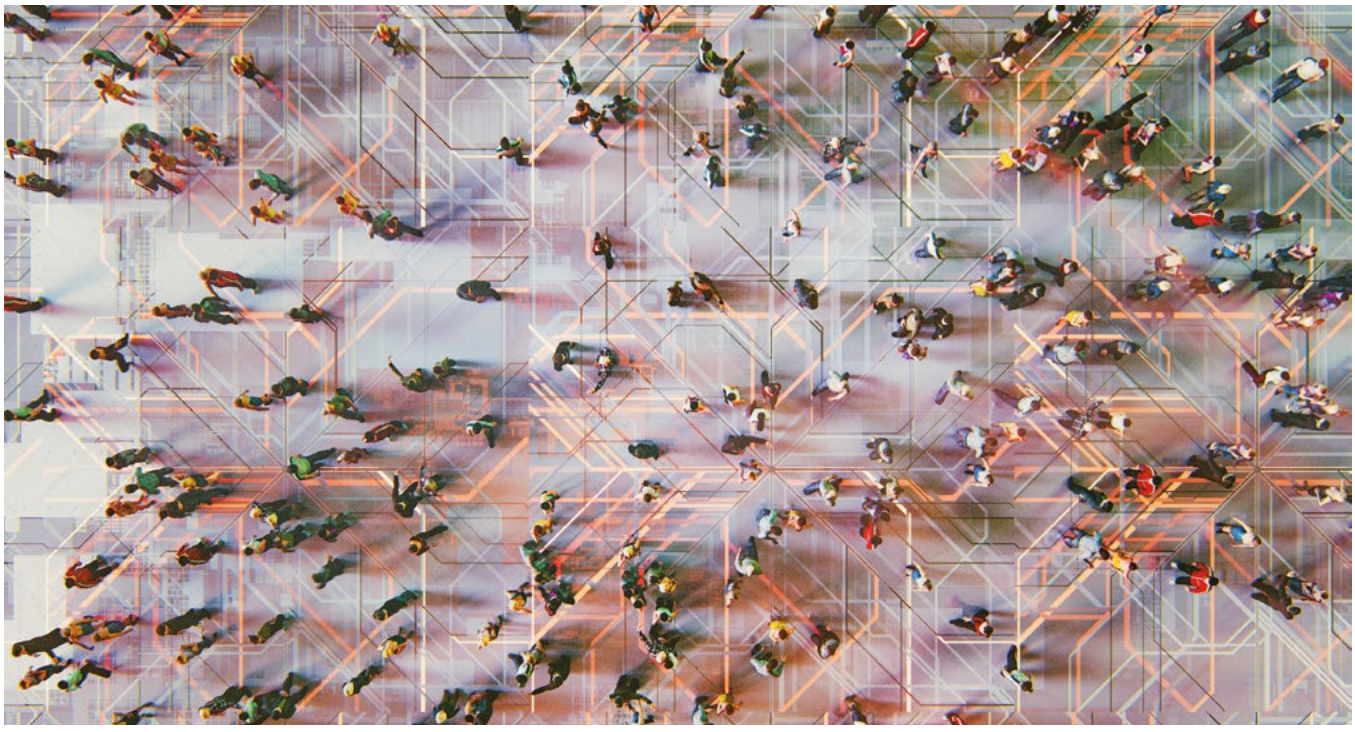
Finally, on May 17, 2024, the California Civil Rights Council announced a notice of proposed rulemaking to prevent discrimination due to the use of AI in employment decisions.

Takeaways

The legal landscape surrounding the regulations for employer use of AI in employment decisions is rapidly changing. Employers must ensure that their use of AI complies with current law. Employers are encouraged to consult their legal counsel to assess whether their use of AI complies with federal, state, and local law.

Holly H. Williamson
Partner, Houston

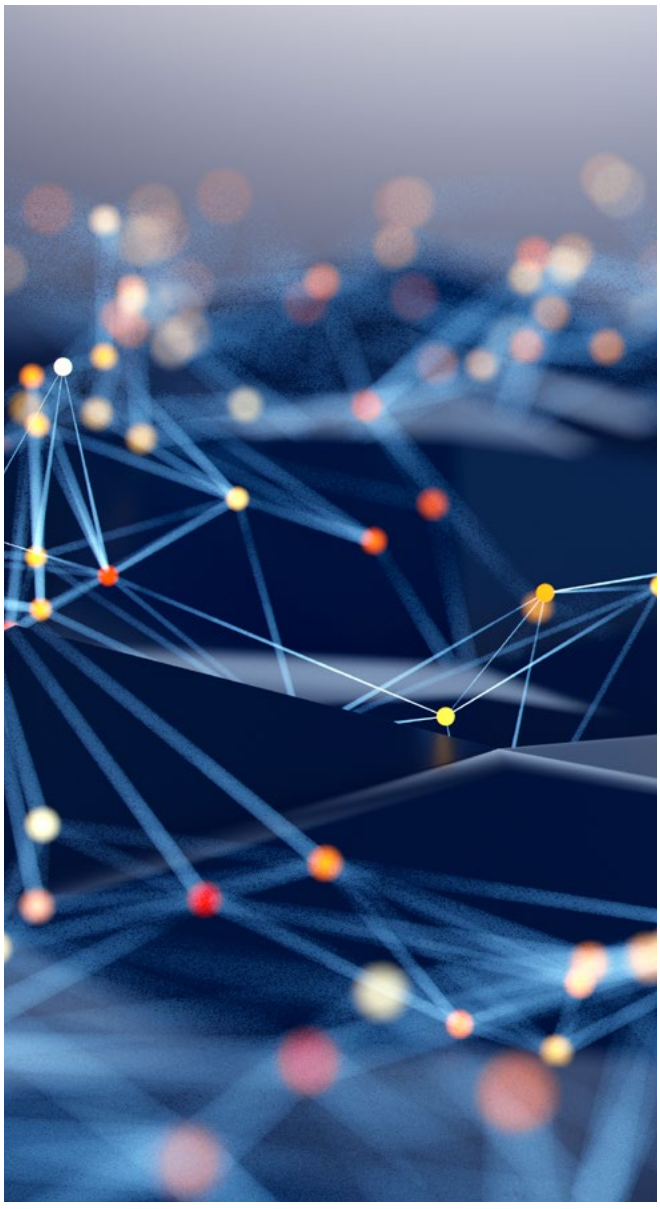
Alyce Ogunsola
Associate, Atlanta



INSURANCE

Navigating AI Disclosures in Insurance Applications: Best Practices for Businesses

Artificial intelligence (AI) is transforming industries at an unprecedented pace, and the insurance industry is trying to keep up. As AI integrates into business operations, from customer service to facilities management to supply and distribution to internal processes and business management, the risks associated with AI increase dramatically. And as risk increases, so too does insurer scrutiny. Such is becoming the case with AI. This article explores the unique challenges in assessing AI risk particularly when it comes to answering questions about AI on insurance applications, and potential best practices for mitigating associated risks.



AI Questions on Insurance Applications

As businesses integrate AI into their operations, insurers are starting to develop targeted questions to assess the associated risks. These inquiries often focus on how a company may be using AI and its impact on business functions and revenue. As one example, an application from Philadelphia Insurance Company requires applicants to: (1) estimate the percentage of revenue derived from "artificial intelligence software/services" and (2) disclose whether their business uses "Generative AI in producing original content," including for advertising or branding.

While these questions may seem straightforward, answering them accurately can be difficult for businesses given the complexities of AI. For example, the term "artificial intelligence" potentially encompasses various technologies, including machine learning, natural language processing and generative AI. The Philadelphia Indemnity application, however, does not supply a meaningful definition of "generative AI," or even "AI." Without a clear definition in the application itself, businesses may struggle to determine which operations even qualify as AI for purposes of responding to the insurer's questions. Insurers may also fail to specify critical parameters such as timeframes for reporting AI usage or whether they seek disclosures about third-party AI systems, services or practices. These ambiguities, combined with the rapid evolution of AI technologies, which may cause even the most accurate responses to quickly become stale, can create challenges for businesses applying for insurance.

The Importance of Accurate Disclosures

In this dynamic environment, the stakes for accuracy in disclosures is high. Depending on how disclosed information bears on a future loss, an incomplete or inaccurate response about the prospective insured's use of AI could result in claim denial or, worse, policy rescission. Given these risks, businesses should adhere closely to best practices when facing renewal or application questions concerning AI:

- **Define AI in a Business-Specific Context:** Given the breadth of the term "artificial intelligence" and the lack of any universally accepted definition, businesses should work with their insurers and brokers to reach a meaningful and functional definition of AI. The agreed definition can be supplied by addendum to the application and can specify the types of technologies and processes that will be considered AI for purposes of that particular business. This proactive clarification

can help align the business's understanding with the insurer's understanding, potentially minimizing coverage disputes.

- **Engage All Stakeholders:** Unlike common-place risks like fire and flood, and liabilities like environmental, products, employment and management, understanding and quantifying the risk that AI poses to a particular business is likely beyond the reach of dedicated risk management personnel. To fully appreciate the risk posed by AI requires input from all aspects of a business. For instance, human resources may use AI to screen employees or monitor behaviors, supply and distribution may use AI to assist with product and product routing, production may use AI across its automated facilities and production lines, and management may use AI to provide strategic advice. In fact, it was recently announced that a company in the United Arab Emirates appointed an AI-powered observer to its board of directors. This follows a Finnish company that named an AI entity to its leadership team and a Hong Kong-based company that appointed a computer algorithm to its board of directors in 2014. Given these broad and varied uses of AI, it is important for businesses to engage all units and stakeholders when it comes to assessing the company's use of AI and, thus, the risk posed by AI.
- **Clarify Third-Party AI Usage Limitations:** Many businesses rely on third-party vendors or partners that incorporate AI into their services. Since businesses often lack full visibility into these third parties' internal operations, businesses may wish to clarify this limitation when answering questions about AI on insurance applications. That is, prospective insureds should make reasonable inquiry to third-party vendors and partners about their use of AI and include such information on their insurance application. Where a company is unable to obtain the information after reasonable inquiry, it should so state. This could protect the business from potential coverage disputes should undisclosed third-party AI cause or contribute to a loss.
- **Provide Date-Specific Information:** Given the rapid pace of AI innovation, businesses should cabin AI-related disclosures to a specific timeframe. In doing so, businesses can avoid accusations that later changes to AI systems or processes render their prior disclosures inaccurate or misleading. In addition, businesses should be explicit about any duties to periodically update the insurer regarding the use of AI during the policy period.

Conclusion

As businesses become more dependent upon the use of AI, insurers are certain to increase their inquiries about it when it comes to the procurement of insurance. Businesses should be on the lookout for AI policy endorsements, provisions and, importantly, questions about AI in insurance applications. As with all insurance application information, accuracy about AI is critical and businesses, therefore, must ensure that their insurance procurement team is fully informed about the business's use of AI and adhere closely to industry best practices when making any AI disclosures.

Michael S. Levine
Partner, Washington, DC and New York

Latosha M. Ellis
Counsel, Washington, DC

Alex D. Pappas
Associate, Washington, DC

PRIVACY AND CYBERSECURITY

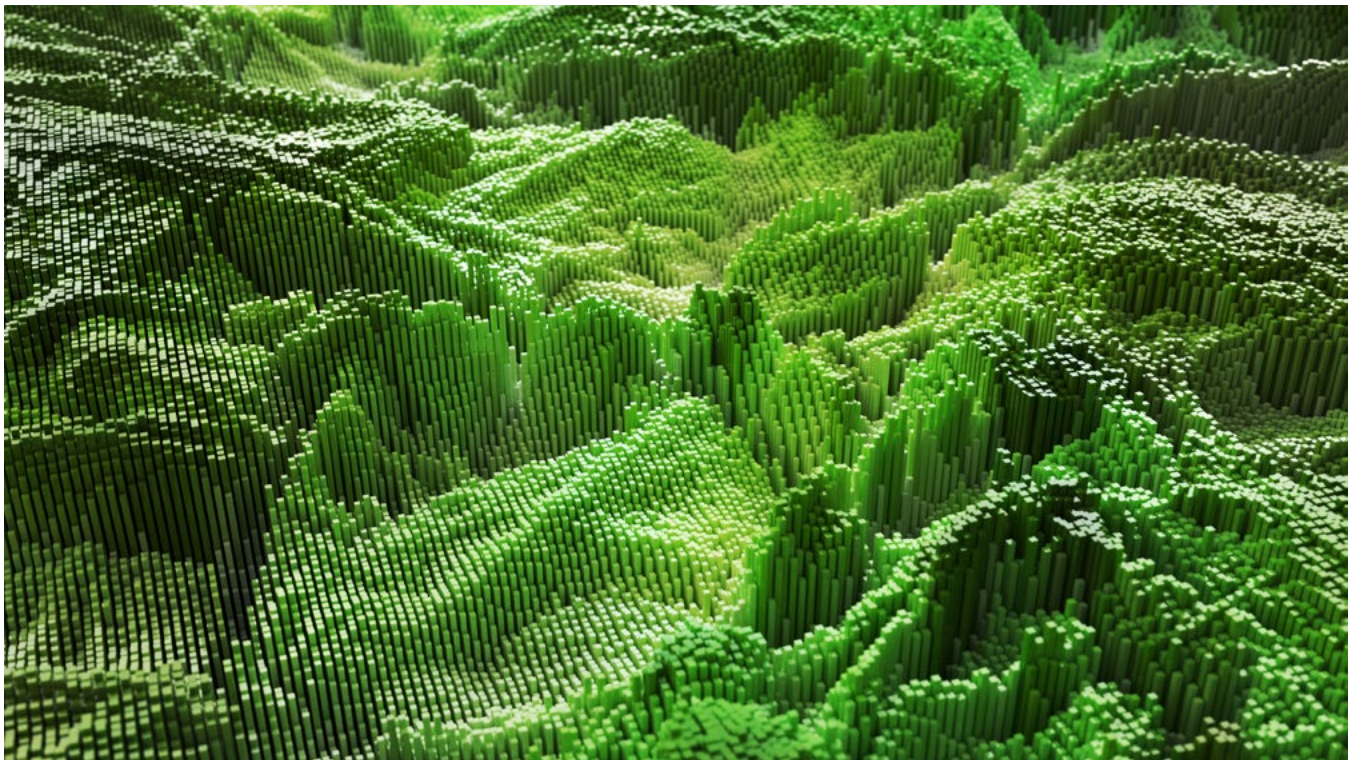
CA Governor's Veto of AI Safety Bill: Where Does US AI Regulation Go From Here?

With California's Governor Newsom's recent veto of Senate Bill 1047 (the Safe and Secure Innovation for Frontier Artificial Intelligence Models Act) (SB 1047), the path forward for comprehensive AI regulation in the US remains uncertain.

SB 1047

Unlike the EU AI Act, which focuses on specific types and applications of high-risk AI systems, SB1047 focused on models that are trained using a significant amount of computing power at a cost of over $100 million. The bill would have required developers of such large-scale, highly advanced frontier models to take a number of steps to prevent both their model and derivatives of their model from being used to enable certain critical harms to public safety and security, including (1) implementing a detailed safety and security protocol; (2) implementing a "kill switch" that enacts a full shutdown of the covered model's operations; (3) conducting safety assessments; (4) reporting safety incidents to the California government; (5) undergoing annual third-party audits; and (6) submitting annual certifications of compliance. "Critical harms" would have included any of the following harms caused by covered models: (1) the creation of weapons of mass destruction in a manner that results in mass casualties; (2) mass casualties or at least $500 million in damage resulting from cyberattacks on critical infrastructure by a model; (3) mass casualties or at least $500 million in damage resulting from a model that acts with limited human oversight and results in death, great bodily injury, property damage, or property loss; or (4) other grave harms to public safety and security.

Governor Newsom ultimately vetoed the bill just before the legislative decision deadline, noting that while California has a responsibility to regulate the AI industry, and the bill was "well intentioned," it nonetheless raised a number of concerns. While SB 1087 received support from a diverse set of stakeholders, the bill also received intense pushback on a number of fronts. The governor cited several objections in his veto letter, such as the threat of stifling innovation in California's AI industry and the bill's focus on large-scale models (based on computing power and cost) rather than AI systems with high-risk applications, regardless of size (e.g., systems involving critical decision-making or sensitive data). Many industry stakeholders also expressed concern that the bill would hold developers liable for downstream actors who use or modify their model in nefarious ways, and argued that this liability regime could negatively impact how models are designed and made available, particularly open-source models.



Where Does US AI Regulation Go From Here?

While the prospect of federal AI legislation remains muddled, particularly in the post-election landscape, there continues to be a flurry of activity at the state level, with state legislatures around the country introducing hundreds of AI-related bills over the course of this year. That said, given the lack of consensus over how to most effectively regulate AI and the pushback from industry stakeholders on rules that may stifle innovation, states will continue to face an uphill battle to pass comprehensive AI legislation. Given these dynamics, in the near term, AI bills that have the highest likelihood of success will likely be those that are narrowly tailored toward specific issues or risks raised by AI rather than those that try to regulate AI more holistically. Nowhere is this more apparent than California where the governor recently signed at least 17 bills related to AI regulation despite vetoing SB 1047. The enacted bills generally focus on specific AI issues (e.g., protections against deepfakes, transparency and reporting obligations, protections for performers and deceased celebrities) or regulate the use of AI in certain sectors (e.g., health care and education). For example:

- The CA AI Transparency Act, effective January 1, 2026, will require providers of publicly accessible generative AI systems with over one million monthly visitors or users to make an AI detection tool available that allows users to assess whether content is AI-generated, among other requirements.
- The CA Generative AI Training Data Transparency Act, effective January 1, 2026, will require developers of generative AI systems to post detailed information on their websites regarding the data used to develop and train their AI systems.
- The CA Healthcare Services: Artificial Intelligence Act, effective January 1, 2025, will require certain healthcare facilities and practices that use generative AI to send patient communications relating to clinical information to include a disclaimer that the communication was generated by AI and instructions for contacting a human (there is an exception for communications read and reviewed by a human licensed or certified health care provider).

California's success with narrowly tailored laws is likely indicative of how similar legislative efforts may play out in other states. Much like data privacy regulation in the US, absent a comprehensive federal law, we should expect to see a growing and complex patchwork of state laws regulating AI for the foreseeable future.

Michael La Marca
Partner, New York

Jennie L. Cunningham
Associate, New York

White House AI Memo Addresses National Security and AI

On October 24, 2024, the White House released a memorandum (the Memo) implementing Executive Order 14110 (EO), titled "Safe, Secure, and Trustworthy Artificial Intelligence," which was issued in October 2023. The EO outlined a comprehensive, all-of-government approach to developing an AI governance framework. The Memo provides further directives related to AI governance, particularly in the national security context.

EO 14110 directed agency action in a range of areas related to AI, including competition and innovation, safety and security, consumer protection, workers' issues, privacy, equity and civil rights, US leadership abroad, and responsible government use of AI. The Memo builds on these themes and outlines three main objectives: (1) advancing the US's leadership in AI; (2) harnessing AI to fulfill national security objectives; and (3) fostering the safety, security, and trustworthiness of AI. The Memo directs a number of agencies, including DOD, DHS, DOE, DOJ, CFIUS, NIST, and others to achieve the Memo's objectives. Highlights include the following:

- **US Leadership in AI:** Ensure the US remains the top location for global AI talent and computing facilities while protecting US AI from foreign intelligence threats.
  - **Promote progress, innovation and competition:** The Memo directs agencies including DOD, DHS, NSF, and DOE to take actions such as streamlining the visa process and fostering investment in AI infrastructure.
  - **Protect industry, civil society, and academic AI intellectual property and infrastructure from foreign intelligence threats:** The Memo directs the NSC and agencies including ODNI, DOD, DOJ, CFIUS, and others to take actions such as reviewing the national security framework doctrine, identifying vulnerabilities in the AI supply chain, and considering AI implications for covered transactions.
  - **Manage risks:** Continue to develop international AI governance with a range of partners. The Memo directs NIST and the Department of Commerce (via NIST's AI Safety Institute) to take the lead in facilitating and providing guidance on AI testing programs and methods.
- **AI and National Security:** Responsibly harness AI's power to meet national security objectives.
  - **Enable effective and responsible use of AI:** The Memo establishes a working group to address issues associated with government procurement of AI. The initiative includes items such as simplifying certain procurement processes to allow more companies to compete for government contracts and directs agencies to prioritize the "technical capability of vendors" in the assessment stage. The Memo further lays out mandates for agencies to engage with a diverse range of stakeholders on AI capabilities, determine which foreign states might be appropriate partners to co-develop AI

and AI assets, revise policies and procedures to address data-related issues, and issue guidance on interoperability across AI functions in the national security space.

  - **Strengthen AI governance and risk management:** The Memo directs relevant agencies to consider specific risks directly related to each agency's use of AI and establish an AI Framework for the national security community.

- **Safe, Secure, Trustworthy AI:** Continue to develop a "stable and responsible" framework for global AI governance. The Memo directs the State Department, in coordination with DOD, the Department of Commerce, DHS, the US Mission to the UN, and USAID to develop a strategy for engaging with global actors on AI governance in accordance with existing frameworks.

The Memo also details the appropriate use of AI in government, with a range of directives related to assessment and reporting across agencies, including a classified annex that covers other sensitive national security issues like countering adversary uses of AI. The Memo states that the recent "paradigm shift" in AI toward large language models and "computationally intensive systems" primarily has occurred outside of government to date, but that it is critically important for the government to assume a key role in AI governance and innovation.

While the Memo's directives, and EO 14110 more broadly, are targeted at government agencies, they nonetheless have certain downstream impacts on the private sector. For example, in the near term, several government bodies are charged with assessing the private sector's competitive advantage in the AI space and risks to that position. The defense and intelligence agencies also are tasked with engaging with private sector stakeholders "on an ongoing basis" to identify emerging capabilities relevant to the US's national security mission. More broadly, EO 14110 directed agencies to take actions impacting the private sector, including issuing regulations and guidance that apply to large swaths of the private sector. In addition, pursuant to EO 14110, the Biden Administration invoked the Defense Production Act to require developers of frontier AI models to disclose the results of their pre- and post-deployment testing exercises, including the results of red-team safety tests. To that end, the Department of Commerce has requested various disclosures from certain companies regarding testing and other issues, and its Bureau of Industry and Security (BIS) issued a proposed rule in September to require quarterly reporting related to (1) the development, training or production of dual-use foundation models; (2) the model weights of those models; (3) the results of red-teaming and other testing; and (4) other information relevant to the models' safety, reliability and risks related to national security. With the first of the Memo's many directives due within 30 days of the Memo's release, and others following at various intervals, the impact of EO 14110 on the private sector could continue to evolve.

That said, from a long-term perspective, the future impact of the Memo and EO 14110 as a whole is unclear, as it has been reported that President-elect Trump plans to repeal EO 14110 upon taking office. While the Trump Administration will likely continue the focus on AI innovation and national security objectives (e.g., export controls on AI technology), it is generally expected that the administration will scale back the federal government's role in certain other areas of AI regulation, such as EO 14110's focus on algorithmic discrimination and the requirement that developers of frontier AI models disclose the results of testing exercises. There are many factors at play in this space, and we continue to monitor ongoing developments related to AI regulation.

Michael La Marca
Partner, New York

Jennie L. Cunningham
Associate, New York

LITIGATION

NYDFS Issues Industry Guidance on AI and Cybersecurity Risks

In October 2024, the New York Department of Financial Services (NYDFS), the state agency responsible for regulating financial services and products in New York, issued an Industry Letter exploring the relationships between artificial intelligence (AI) technologies and cybersecurity risk management. The Letter is a direct response to inquiries that NYDFS has received regarding the effects of advancements in AI technologies on cybersecurity risk and ways in which companies can mitigate this risk.

The NYDFS notes that advancements in AI technologies have enabled bad actors to engage in increasingly complex social engineering through the use of "deepfakes"—realistic text, audio, and even video messages targeted at employees to convince them to disclose sensitive and confidential information. The NYDFS also observed that cybercriminals may use AI to identify and exploit security vulnerabilities, spread malware, and exfiltrate sensitive data much faster than can be accomplished by a human.

The Letter also highlights how companies using AI technologies may be subject to unique risks. These technologies typically require large amounts of data to improve their reliability, and the collection and processing of this data creates an attractive target for bad actors. Many such technologies further require the involvement of third-party vendors and service providers, creating additional opportunities for potential cybersecurity exposure.

The NYDFS points to the agency's cybersecurity regulation, 23 NYCRR Part 500, as a framework for assessing and responding to these risks. For example, the regulation requires companies to maintain cybersecurity programs and policies based on risk assessments, which should include both defensive measures against third-party misuse of AI and proactive directives on a company's own use of AI technologies. The NYDFS further directs companies to ensure that third-party service provider policies require due diligence before permitting third parties to access sensitive and confidential data and that this procedure evaluate potential AI-related threats facing third-party providers. Finally, the NYDFS identifies a suite of other defensive measures common in the cybersecurity space, such as access controls, cybersecurity training, active monitoring, and data management policies.

We also reported on the Industry Letter on Hunton's Privacy & Information Security Law Blog.

Litigation involving AI issues has risen steadily since 2018, with a record number of AI-related lawsuits filed just last year, according to the Hunton Andrews Kurth Emerging Technologies Tracker. This year is shaping up to be another record breaker in terms of newly filed AI litigation, demonstrating the importance of ensuring that companies using AI comply with constantly evolving federal and state statutory and regulatory guidelines.

Nicholas Drews
Associate, Washington, DC

Torsten M. Kracht
Partner, Washington, DC
and New York

HUNTON
ANDREWS KURTH