INSTITUTE FOR HOMELAND SECURITY

Regulating Artificial Intelligence in the State of Texas: Challenges and Opportunities

Institute for Homeland Security

Sam Houston State University

Alexander Kinney Ph.D

Sam Houston State University™

ABSTRACT

Developing a comprehensive regulatory approach for artificial intelligence remains a challenging prospect. In recent years, several states have moved to implement such frameworks. With the passage of the Texas Responsible Artificial Intelligence Governance Act (TRAIGA) in June of 2025, Texas established itself as a leader in this effort. The act aims to balance the need to promote innovation through artificial intelligence with the need to mitigate risk. Unsurprisingly, the intentions of this policy have deep implications for critical infrastructure resilience. The aim of this technical paper is to evaluate the potential impacts of this new policy on AI governance, review its potential impact on businesses operating in critical infrastructure sectors, and highlight opportunities for strengthening this foundational piece of legislation. In what follows, I will provide a brief overview of the significance of regulating AI development and misuse, review the risks associated with AI misuse, and describe complementary state-level efforts to regulate AI that have been enrolled into law. I will then provide an overview of TRAIGA and suggest several ways that future legislative efforts can improve on the provisions outlined in this act.

Table of Contents

INTRODUCTION & OVERVIEW 1

PROBLEM STATEMENT 2

Research Objective 3

TOPIC DISCUSSION 4

Taxonomy of Stakeholder Risks 4

Taxonomy of Causal Risks 6

Setting the Stage: Key AI Governance Frameworks Shaping Texas Policy 7

A WAY FORWARD 11

The Texas Responsible Artificial Intelligence Act (TRAIGA) 11

Building on TRAIGA to Improve Critical Infrastructure Resilience 12

CONCLUSION 14

REFERENCES 15

AUTHOR BIOGRAPHY 18

INTRODUCTION & OVERVIEW

Background and Significance of Regulating AI development and Misuse

There has been a dramatic increase in the deployment of artificial intelligence (AI) systems over the past decade. These systems have reshaped everything from the consumer experience to finance, logistics, and defense (Cath, 2018). There are notable risks associated with the haphazard rollout of these systems, which presents unique governance challenges. AI has become infused in nearly every aspect of society, and when misused, this technology has the potential to threaten public safety on a domestic and international scale (UNESCO, 2023). Moreover, uncritical adoption of AI has been shown to upend organizational operations (Laplante & Amaba, 2021). As a result, there are few issues more pressing for policymakers than developing a comprehensive regulatory framework to govern AI development and use; one that will adequately mitigate risk without stifling corporate innovation and competitiveness.

The urgency of addressing these issues is magnified by the rapid pace with which AI is becoming an essential operational feature of critical infrastructure sectors including healthcare (Topol, 2019) and power grid management (Irving, 2025). The speed of development and deployment of AI systems has also been unprecedented in recent times. With a mixture of publicly and privately funded efforts to develop this tech, transparency in the research and development process is mixed (Lichfield, 2025). This poses additional barriers to effective policymaking because the complexity of these systems may elude traditional avenues of oversight. Moreover, because of their dynamic nature, AI systems are uniquely vulnerable to failures that are not easily anticipated even by their creators (Munz, Hennick, & Stewart, 2023).

The above challenges are especially alarming for organizations operating in critical infrastructure sectors, where failing to account for risk can be catastrophic. Critical infrastructure organizations are disproportionately targeted by cybercriminals (Adebayo, 2025). Moreover, the resilience of these sectors relies on clear and consistent regulatory guidance (Yigit et al., 2024). It also depends on the organizational ability to deploy AI systems in a manner that allows them to remain competitive and efficient. Despite this, the policy landscape continues to evolve at a glacial pace as compared to

the advent of new AI technology. This creates a critical need for translational research aimed at guiding regulators in their efforts to develop actionable policy that will promote ethical and effective AI use.

PROBLEM STATEMENT

Today, critical infrastructure organizations and operators are navigating an uncertain and rapidly changing AI governance landscape (Chrichton et al., 2024). How this unfolds in the coming years will have a deep impact on the management and protection of infrastructure systems and have downstream impacts on public safety. Resolving questions surrounding what rules to apply, who will be responsible for enforcing them, and how compliance will be measured will have downstream effects on what role AI plays in bolstering, or alternatively undermining, critical infrastructure resilience. Despite the importance of addressing these issues, AI governance remains fragmented in the United States. Federal agencies have issued piecemeal guidelines, but the AI policy landscape is primarily developing through a series of regulatory frameworks that are emerging at the state-level. Each of these frameworks takes a different approach to balancing the need to mitigate risk against the need to support innovation (Horwitch, 2024). This means that on the ground, compliance expectations differ for businesses depending on which jurisdiction they operate within. Furthermore, the federal government has taken increasingly bold steps to challenge the validity of state regulations without offering a holistic national framework (Miller & Bordelon, 2025). In this void, state governments still shoulder the responsibility of innovating best practices that may, or may not, become obsolete as the regulatory environment evolves in the future. Without addressing these issues, states risk implementing frameworks that are unable to anticipate developments in AI technology leaving them unprepared for addressing potential harms.

Research Objective

In June 2025, legislators in Texas took a leading role in this effort with the passage of HB 149, otherwise known as “The Texas Artificial Intelligence Governance Act” or “TRAIGA.” TRAIGA represents a significant step forward in codifying a set of uniform principles for AI use and is notable for several reasons (see Vital & Clark, 2025). First, it leans more toward a set of targeted provisions rather than a broad form rules-package. Second, in its enrolled form, it represents a pared down approach to AI governance in lieu of more expansive earlier drafts. Finally, it diverges from other comprehensive frameworks employed in other states in meaningful ways that could yield several potential benefits and drawbacks. In what follows, this paper will situate the impact of TRAIGA with respect to critical infrastructure governance. It begins by contextualizing the nature of AI misuse, covering system and human factors that can lead to adverse outcomes. It then reviews existing approaches to AI governance in the U.S., with particular attention devoted to leading approaches at the state-level. As a part of this section, the paper will outline key provisions in TRAIGA. Finally, this paper will offer several recommendations for strengthening TRAIGA in future legislative sessions to better position Texas in the national conversation on the best practices for regulating AI.

TOPIC DISCUSSION

Toward a Unified Language for Classifying Artificial Intelligence Risk

While the broad capability of AI holds immense potential to shepherd in a new era of efficiency and capability in virtually every facet of social life, the diversity of AI applications also introduces a diverse set of novel threats while reinforcing existing ones (Slattery et al., 2024; Zeng et al., 2024). Efforts to categorize AI risks have been piecemealed, with several taxonomies proposed by academics, industry insiders, and government agencies. Recent attempts to synthesize these taxonomies into a working framework have been fruitful. Zeng et al.'s (2024) metanalysis of existing benchmarks proposes a unified AI Risk Taxonomy (AIR 2024), that partitions identified risks into four distinct categories:

1. System & Operational Risks
2. Content Safety Risks
3. Societal Risks, and
4. Legal & Rights-Related Risks.

Moreover, Slattery et al., (2024) suggest that when and why risks occur from AI can be further grouped according to:

1. The entity interfacing with AI
2. The intent behind AI use, and
3. The timing of AI deployment.

This section reviews these risk categories and their pertinence to critical infrastructure sectors. Collectively, they provide a way to account for risk in the context of both stakeholder interests and causality.

Taxonomy of Stakeholder Risks

<u>System & Operational Risks</u>

There are several technical risks associated with AI use that relate to AI system design itself. These include issues of algorithmic bias where systems are developed using

biased data, unintended consequences, and where systems that are assumed to be correctly designed produce inconsistent outputs. Technical vulnerabilities embedded in these systems may not be easily identified until after a breakdown occurs. These vulnerabilities can lead to security risks within organizations that compromise the integrity of other organizational systems or send critical systems offline. They can also undermine operational efficiency and worker safety. Operational misuse of AI can lead to unsafe operation of systems that can threaten public safety. In the context of critical infrastructure, system and operational risks can misclassify threats, lead to misprioritized resources, or even lead to the failure of existing emergency protocols.

Content Safety Risks

AI systems are also capable of producing or amplifying harmful content. Though it is more common to hear about this category of risk in the context of consumer-facing platforms like social media, critical infrastructure sectors are not immune to the content safety risks. Large language models that are used to generate operational guidance may produce unsafe recommendations. Elevating this concern is the speed and scale with which AI has been implemented. There is emerging evidence that people are willing to rely on AI systems to a fault, misplacing trust in AI generated recommendations (Bucinca et al., 2021). Moreover, AI systems have the capability of producing illicit content that could introduce organizational liability.

Societal Risks

AI systems carry several notable societal risks including the capability to engage in political/economic harm, deception, and manipulation. These types of risks carry several potential consequences in an organizational context. AI has the potential to disrupt the labor process, to engage in unfair market practices, and misrepresent information. Likewise, they can unintentionally flout compliance processes that are put in place by policymakers without diligent oversight. These types of risks could lead to a wholesale disruption of critical infrastructure sectors, and are particularly difficult to mitigate (Zeng et al., 2024).

Legal & Rights Related Risks

There is notable legal, and rights-related risks associated with the use of AI systems that warrant further consideration. AI has the potential to facilitate unlawful activities of a criminal and civil nature. These activities include discrimination against members of protected classes, unauthorized collecting and sharing of sensitive data, leaking trade secrets, and surveillance. Likewise, AI systems can be a vector for cybersecurity threats that could undermine national security or government interests (Zeng et al., 2024).

Taxonomy of Causal Risks

Entity

Entity refers to who is responsible for introducing risk in AI use (Slattery et al., 2024). There are distinct risks from human decisions or actions in AI development or deployment. This can include poorly training the system or improperly using AI beyond its intended function. These are distinct from risks that can be attributed to AI itself, such as undermining the ability for humans to make essential decisions. There are also outsider threats to (e.g., “other”) where risk is caused by a reason that is ambiguous or due to the inherent complexity of the AI system.

Intent

Intent captures the degree to which risk is an expected or unexpected aspect of AI use (Slattery et al., 2024). Intentional risks reveal themselves when AI deliberately causes harm in the pursuit of a goal. For example, an AI system could be intentionally programmed to conduct a DDOS attack against a government, healthcare, or financial services agency. Unintentional risks could be associated with improper development, such as unknowingly using biased training data in AI system development. Like entity-related risk, there is the potential for risk to be neither intentional or unintentional, such as cases where AI intentionally or unintentionally infringes upon privacy depending on how the system is being used.

Timing

Finally, timing captures where risk can be attributed based on the lifecycle of AI system development and deployment (Slattery et al., 2024). Risks can present themselves pre-deployment. Examples of pre-deployment risks include coding errors during system development. They can also present themselves post-deployment, such as the misuse of AI systems for harmful purposes. It is worth noting that it is not always easy to categorize risks in the AI lifecycle. Other timing risks include the known issue with AI system energy consumption that could present issues either pre- or post-deployment depending on the context.

Setting the Stage: Key AI Governance Frameworks Shaping Texas Policy

As it currently stands, U.S. congressional leaders have yet to implement a comprehensive federal regulatory framework for AI despite a clear recognition that more needs to be done to address the societal, technical, and operational risks of this evolving technology (Phillips-Robins and Singer, 2025). Without congressional action, the task has fallen to state legislatures across the country to innovate AI governance on a more localized level and they are looking abroad to the European Union as a model for domestic policy development (Turner Lee and Stewart, 2025). All 50 states, Puerto Rico, the Virgin Islands, and Washington D.C. either have enacted or pending legislation on this topic (National Conference of State Legislatures, 2025). Currently, only Colorado, Texas, and Utah have developed unified comprehensive AI regulatory frameworks. Policy observers also tend to pay attention to legislative efforts in California as the state is seen as a vanguard of AI governance (Kohler, 2025). These approaches to AI governance exhibit synergies and divergences in a cross-jurisdictional context. They also demonstrate that the notion of “risk” varies across state frameworks.

European Union

The passage of the European Union's "Artificial Intelligence Act" (EUAIA) has placed a great deal of pressure on U.S. lawmakers to pass comprehensive AI legislation (Gracias, 2024). Though executive action has been taken on this issue, a binding legislative package remains out of reach. This has led many state legislatures to seek inspiration for domestic AI governance provisions from the EUAIA as it is the first comprehensive legal framework that has global implications (Ayoub, Copeland, and Jiva, 2025). The EUAIA takes a categorical approach to classifying risk, but is less sensitive to implementing adaptable provisions to account for whether AI systems pose minimal, limited, high, or even unacceptable risk to public safety. These risk classifications are broken down as follows:

1. Unacceptable risk: Applications of artificial intelligence that include biometric surveillance of public spaces in real time, exploitation of minors, social scoring, and/or emotional-behavioral manipulation.
2. High risk: AI systems that impact critical infrastructure sectors. These AI systems are subject to demanding requirements to manage risk, audit data, provide transparency, document activity, and are subject to continuous monitoring obligations.
3. Limited risk: Mostly concerns content generation platforms (e.g., ChatGPT/Grok etc.). AI-generated content is subject to labels, and systems must meet certain transparency metrics.
4. Minimal risk: Most daily applications of AI (e.g., email filters, spellcheck, etc.). No additional regulations.

Beyond provoking domestic legislative attention, the EUAIA has direct implications for critical infrastructure organizations operating in the United States as many AI systems, which are adopted in these sectors, are considered high-risk. Healthcare organizations are required to audit their own AI systems for compliance with this act, or they could lose access to the EU market. Manufacturers and organizations in the financial services sector are also subject to similar compliance obligations and must conform to the EUAIA's transparency standards.

California

The state of California has been at the forefront of regulating AI. Rather than approach the issue through a single bill, California has enacted AI governance through multiple complementary pieces of legislation that are tailored to specific risks associated with AI development and use (Anderson, Reem, and Tadayyon, 2024). These pieces of legislation are wide ranging, touching on everything from safety, consumer protections, reporting accountability, and privacy. In 2024 alone, the California State Legislature enacted 17 laws related to AI (Baer and Rubenstein, 2025). Specific legislative efforts have directly tied to critical infrastructure. Notably, AB-3030 or the "Health Care Services: Artificial Intelligence Act" regulates how health facilities including hospitals, physician's offices, and clinics incorporate generative AI into standard operating procedures. Likewise, SB-1120, otherwise known as the "Health Care Coverage: Utilization Review" requires health care providers to inform patients when AI systems are used to manage patient data. SB-896, also known as the "Generative Artificial Intelligence Accountability Act" directs state agencies to conduct regular assessments of generative AI risk and report on potential mass casualty events to the state legislature. Finally, AB 2013 or the "Generative Artificial Intelligence Training Data Transparency Act" requires developers of AI algorithms to disclose the data used to create AI systems, potentially providing critical infrastructure organizations greater insight into which models are suitable for their needs. Enforcement is spread out through a combination of state agencies, and violations can carry either criminal or civil penalties.

Colorado

Colorado has approached AI governance in a more holistic manner. Enacted in May of 2024, S.B. 24-205 known colloquially as the "Colorado Artificial Intelligence Act (CAIA)" wraps AI regulations into a singular piece of legislation. Though it will not go into effect until 2026, the act primarily targets "high-risk" AI systems that are designed for predictive use, rather than content generation (Siegal and Garcia, 2024). The CAIA adopts a similar definition of "high-risk" AI to the EUAIA. Any system that plays a critical

role in making a “consequential decision,” or a decision that influences the operations or costs associated with critical infrastructure sectors, is considered high-risk (Levi et al., 2024a). The CAIA also imposes several obligations on developers and adopters of high-risk AI systems regarding transparency, risk analysis, and approaches to mitigation if they are to be deployed in these sectors. It is notable that the CAIA outlines several exemptions for certain developers and adopters if they automatically meet employment thresholds or release impact assessments to the public. The CAIA also follows draft regulations that were implemented in California regarding consumer privacy (see Siegal and Garcia, 2024). Under the CAIA, enforcement is exclusively under the purview of the Colorado Attorney General and carries only civil penalties for violations. The CAIA also does not provide the ability for private parties to sue to enforce the law. All actions must be initiated through the Attorney General.

Utah

Utah was the first state to enact a comprehensive AI governance framework (Levi et al, 2024b). SB-149 or the “Utah Artificial Intelligence Policy Act (UAIPA)” imposes disclosure requirements on entities that intend to use generative AI when interfacing with customers. It also takes a bold step in limiting the ability of entities to blame AI if AI makes statements or acts in an official capacity on their behalf should they constitute a violation of consumer protection laws. Unlike Colorado, the UAIPA is specifically focused on content producing AI systems, not predictive systems. Instead of taking the tact of outlining specific sectors that are implicated by the law, the UAIPA instead specifies “regulated occupations” that are subject to the provisions it outlines. These occupations are those that require state certification or a state-issued license to practice. This implicates some organizations and employees in critical infrastructure sectors, namely healthcare professionals. Under the UAIPA, enforcement is under the purview of the Utah Division of Consumer Protection (UDCP) and primarily outlines civil penalties. Likewise, the UAIPA does not provide the ability for private entities to sue for enforcement. Unlike California and Colorado, the UAIPA implements a “regulatory sandbox” to promote innovation which is a policy tool that allows organizations to have

a measured degree of immunity while they develop cutting edge AI systems (e.g., reduced fines for violations/cure periods for when fines are assessed).

A WAY FORWARD

The Texas Responsible Artificial Intelligence Act (TRAIGA)

On January 1, 2026, TRAIGA officially took effect allowing Texas to ascend into a leading role in the national conversation regarding best practices for comprehensively regulating AI. The implementation of this law followed an extended back-and-forth among legislators, prompting multiple rounds of revisions to the text of the bill. As a result, the final version that was enrolled and ultimately signed by Governor Greg Abbott represents a pared back version of the original effort (Parker, Hockaday, and Lewis, 2025). The final law blends key provisions that have appeared in other frameworks domestically and internationally, while also diverging in several ways to account for Texas-specific needs (McGinnis and Carter, 2025). This positions TRAIGA as a first-of-its-kind framework. Like other governance frameworks, TRAIGA prohibits the development or use of AI for the express purpose of criminal activity. Like the framework employed in Colorado, it prohibits the use or development of AI with the intent to discriminate against protected classes, implements similar transparency requirements, and focuses specifically on “high-risk” systems.

However, there are wrinkles in how many of these provisions are implemented that distinguish TRAIGA from its counterparts. Perhaps one of the more controversial, but also most innovative, features is the regulatory sandbox program. This program permits approved participants to test AI systems with exemption from many of the accountability, disclosure, and licensing provisions outlined in TRAIGA (Vital and Clark, 2025). Utah has implemented a similar system, but what sets TRAIGA apart is the broader scope of exemptions outlined. TRAIGA allows businesses to participate in the sandbox program for up to 36 months. While this approach to the regulatory sandbox may promote innovation and inform future policy, there is little existing precedent for these programs.

Oversight and risk management of this program is conducted by a novel council comprised of lawmakers and members of the public (Palomo et al., 2025). The experimental nature of this program has the potential to command significant public resources for monitoring efforts. Some expect that this will create difficulties for smaller businesses (Vital and Clark, 2025), potentially complicating efforts to set consistent industry standards. This surfaces a broader policy tension inherent to leadership through state governance; encouraging responsible forms of experimentation with AI is necessary to realize the full potential of this technology, but efforts must be made to ensure that this environment remains accessible to organizations that differ in size and resources. Working to achieve this balance will be a crucial factor in whether TRAIGA's sandbox model becomes emulated in other jurisdictions.

Following Colorado, TRAIGA also delegates enforcement authority exclusively to the Texas Attorney General and does not permit private entities to sue for enforcement. It outlines several categories of civil penalties for violations. These include up to a $12,000 fine for violations that can be remedied, up to a $200,000 fine for violations that cannot be remedied. Additionally, for continued violations, entities can be fined up to $40,000 per day for violations that are ongoing (Linda Ross, Hollis, and Zhang, 2025). As compared to other state frameworks, the penalties outlined in TRAIGA are notably more aggressive (Parker and Chandler, 2025). The effectiveness of these penalties will hinge on whether they effectively strike a middle ground between deterrence and feasible compliance.

Building on TRAIGA to Improve Critical Infrastructure Resilience

Based on the preceding review, this section identifies five opportunities for future policy to build on the foundation set forth by TRAIGA to better position the future of AI in Texas. These recommendations include:

1. Taking a more granular approach to risk categorization that aligns AI governance with evidence-based research. Specifically, AI governance in Texas would benefit from a classification system that differentiates between low-, medium-, and high-impact applications of AI in critical infrastructure sectors.

2. Monitoring and aligning oversight of the regulatory sandbox program with pending cross-jurisdictional developments. With the rapid evolution of AI policy, the sandbox program could be improved through lessons learned from similar initiatives in neighboring states. This will ensure that Texas remains both an accountable and a competitive environment for AI development.
3. Strengthening oversight and risk prevention by developing incentives for the AI council to issue publicly available reports on the state of the regulatory sandbox program on a periodic basis. Public access to these reports could strengthen collaboration between academic and state stakeholders to provide continual feedback and suggest further improvements to the program.
4. Adjust liability standards to better account for the unique harms that can be introduced by AI system development, deployment, and end-use. More clearly defining liability in these specific areas of AI interaction could reduce litigation by clarifying existing ambiguities, while improving consumer trust and critical infrastructure resilience.
5. Continue to harmonize TRAIGA with emerging state frameworks and evolving federal stances toward state-level AI laws by conducting regular reviews of the national policy landscape.

Collectively, these recommendations create a series of pathways to transform TRAIGA into a flexible governance model that is responsive to local stakeholder needs, while furthering national conversations about how to best regulate AI.

CONCLUSION

The rapid expansion of artificial intelligence technologies across critical infrastructure sectors has introduced both a complex set of risks and unprecedented opportunities. This technical paper demonstrates that though the AI regulatory landscape remains uneven, the Texas state government has taken the lead to innovate solutions while federal action remains out of reach. The Texas Responsible Artificial Intelligence Governance Act (TRAIGA) joins a host of pivotal frameworks seeking to build a regulatory standard, signaling the state's commitment to ensuring that AI development and use follow a set of principles that promote accountability and transparency, while importantly, remaining forward-thinking. As the preceding comparative analysis demonstrates, TRAIGA is a strong starting framework with tailored provisions that respond to Texas's unique economic and regulatory landscape. However, this white paper encourages policymakers to consider several revisions to this framework to meet the evolving needs of stakeholders, particularly those operating in critical infrastructure sectors. By taking key steps to align TRAIGA with evidence-based AI risk taxonomies developed by experts, incorporating additional measures to bolster the regulatory sandbox program, and remaining agile to evolving regulatory developments at the state and federal level, Texas will remain positioned to shape the conversation regarding how to best regulate AI to ensure that future policymaking is responsive to industry needs while promoting resilience.

REFERENCES

Adebayo, K. S. (2025, April 25). *The Answer To AI-Driven Attacks On Critical Infrastructure: Resiliency*. Forbes. https://www.forbes.com/sites/kolawolesamueladebayo/2025/03/25/the-answer-to-ai-driven-attacks-on-critical-infrastructure-resiliency/

Anderson, H., Reem, N., & Tadayyon, S. (2024, October 10). *Raft of California AI Legislation Adds to Growing Patchwork of US Regulation | White & Case LLP*. https://www.whitecase.com/insight-alert/raft-california-ai-legislation-adds-growing-patchwork-us-regulation

Ayoub, M., Copeland, J., & Jiva, S. (2025, June 12). The EU AI Act: What U.S. Companies Need to Know. *Bond, Schoeneck & King PLLC*. https://www.bsk.com/news-events-videos/the-eu-ai-act-what-u-s-companies-need-to-know

Baer, A., & Rubenstein, R. (2025, January 27). *California Passes Flurry of Year-End AI Legislation [Alert]*. https://www.cozen.com/news-resources/publications/2025/california-passes-flurry-of-year-end-ai-legislation

Buçinca, Z., Malaya, M. B., & Gajos, K. Z. (2021). To Trust or to Think: Cognitive Forcing Functions Can Reduce Overreliance on AI in AI-assisted Decision-making. *Proc. ACM Hum.-Comput. Interact.*, *5*(CSCW1), 188:1-188:21. https://doi.org/10.1145/3449287

Cath, C. (2018). Governing artificial intelligence: Ethical, legal and technical opportunities and challenges. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2133), 20180080. https://doi.org/10.1098/rsta.2018.0080

Crichton, K., Ji, J., Miller, K., Bansemer, J., Arnold, Z., Batz, D., Choi, M., Decillis, M., Eke, P., & Gerstein, D. M. (2024). Securing Critical Infrastructure in the Age of AI. *Center for Security and Emerging Technology, October. Https://Doi. Org/10.51593/20240032*.

Gracias, S. (2024). Comparing the EU AI Act to Proposed AI-Related Legislation in the US | The University of Chicago Business Law Review. *The University of Chicago Business Law Review*. https://businesslawreview.uchicago.edu/online-archive/comparing-eu-ai-act-proposed-ai-related-legislation-us

Horwitch, M. (2024). The AI Challenge for National Technology Strategy. *2024 Portland International Conference on Management of Engineering and Technology (PICMET)*, 1–11. https://doi.org/10.23919/PICMET64035.2024.10653430

Irving, D. (2025). *AI and the Future of the U.S. Electric Grid*. https://www.rand.org/pubs/articles/2025/ai-and-the-future-of-the-us-electric-grid.html

Laplante, P., & Amaba, B. (2021). Artificial intelligence in critical infrastructure systems. *Computer*, *54*(10), 14–24.

Levi, S., Kumayama, K., Ridgway, W., Ghaemmaghami, M., & Neal, M. (2024, June 24). *Colorado's Landmark AI Act: What Companies Need To Know*. https://www.skadden.com/insights/publications/2024/06/colorados-landmark-ai-act

Levi, S., Ridgway, W., Simon, D., Slawe, M., & Oh, A. (2024, April 5). *Utah Becomes First State To Enact AI-Centric Consumer Protection Law | Insights | Skadden, Arps, Slate, Meagher & Flom LLP*. https://www.skadden.com/insights/publications/2024/04/utah-becomes-first-state

Lichfield, G. (2025, February 11). *Public AI infrastructure: What is it, do we need it and will it ever be built? A media leader explains*. World Economic Forum. https://www.weforum.org/stories/2025/02/public-ai-infrastructure-a-media-leader-explains/

Linda Ross, S., Hollis, C., & Zhang, A. (2025, July). *Texas Responsible Artificial Intelligence Governance Act*. Https://Www.Insidetechlaw.Com/Blog/2025/07/Texas-Responsible-Artificial-Intelligence-Governance-Act. https://www.insidetechlaw.com/blog/2025/07/texas-responsible-artificial-intelligence-governance-act

McGinnis, K., & Carter, J. (2025, July 3). *A Red State Model for Comprehensive AI Laws: Texas Enacts the Responsible Artificial Intelligence Governance Act.* https://www.mvalaw.com/data-points/a-red-state-model-for-comprehensive-ai-laws-texas-enacts-the-responsible-artificial-intelligence-governance-act

Munz, P., Hennick, M., & Stewart, J. (2023). Maximizing AI reliability through anticipatory thinking and model risk audits. *AI Magazine*, *44*(2), 173–184. https://doi.org/10.1002/aaai.12099

National Conference of State Legislatures. (2025). *Artificial Intelligence 2025 Legislation*. https://www.ncsl.org/technology-and-communication/artificial-intelligence-2025-legislation

Palomo, R., Caine, M., Petro, L. G., & Ewing, G. (2025). *Texas Enacts New AI Law: What TRAIGA Means for Your Business*. https://www.dickinson-wright.com/news-alerts/client-alert-texas-passes-traiga

Parker, A. M. C., & Chandler, K. J. (2025). *Texas Joins Growing State-by-State AI Regulation in Enacting Comprehensive AI System Law*. Benesch, Friedlander, Coplan & Aronoff LLP - Texas Joins Growing State-by-State AI Regulation in Enacting Comprehensive AI System Law. https://www.beneschlaw.com/resources/texas-joins-growing-state-by-state-ai-regulation-in-enacting-comprehensive-ai-system-law.html

Parker, K., Hockaday, B., & Lewis, G. (2025, June 25). *Pared Back Version of the Texas Responsible Artificial Intelligence Governance Act Signed Into Law*. https://www.klgates.com/Pared-Back-Version-of-the-Texas-Responsible-Artificial-Intelligence-Governance-Act-Signed-Into-Law-6-24-2025

Phillips-Robins, A., & Singer, S. (2025, July 10). *The State of State AI Law: What's Coming Now that the Federal Moratorium Is Dead*. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2025/07/state-ai-law-whats-coming-now-that-the-federal-moratorium-is-dead?lang=en

Siegal, A., & Garcia, I. (2024, October 26). A Deep Dive into Colorado's Artificial Intelligence Act. *National Association of Attorneys General*. https://www.naag.org/attorney-general-journal/a-deep-dive-into-colorados-artificial-intelligence-act/

Slattery, P., Saeri, A. K., Grundy, E. A. C., Graham, J., Noetel, M., Uuk, R., Dao, J., Pour, S., Casper, S., & Thompson, N. (2025). *The AI Risk Repository: A Comprehensive Meta-Review, Database, and Taxonomy of Risks From Artificial Intelligence* (No. arXiv:2408.12622). arXiv. https://doi.org/10.48550/arXiv.2408.12622

Topol, E. J. (2019). High-performance medicine: The convergence of human and artificial intelligence. *Nature Medicine*, *25*(1), 44–56. https://doi.org/10.1038/s41591-018-0300-7

Turner Lee, N., & Stewart, J. (2025, May 14). States are legislating AI, but a moratorium could stall their progress. *States Are Legislating AI, but a Moratorium Could Stall Their Progress*. https://www.brookings.edu/articles/states-are-legislating-ai-but-a-moratorium-could-stall-their-progress/

UNESCO. (2023). *UNESCO's Recommendation on the Ethics of Artificial Intelligence*. https://unesdoc.unesco.org/ark:/48223/pf0000385082

Vital, V., & Clark, A. (2025, July 14). *Texas Enters the AI Sandbox with TRAIGA: Implications for Business Trials*. https://www.americanbar.org/groups/business_law/resources/business-law-today/2025-july/texas-enters-ai-sandbox-with-traiga-implications-business-trials/

Yigit, Y., Ferrag, M. A., Sarker, I. H., Maglaras, L. A., Chrysoulas, C., Moradpoor, N., & Janicke, H. (2024). *Critical Infrastructure Protection: Generative AI, Challenges, and Opportunities* (No. arXiv:2405.04874). arXiv. https://doi.org/10.48550/arXiv.2405.04874

Zeng, Y., Klyman, K., Zhou, A., Yang, Y., Pan, M., Jia, R., Song, D., Liang, P., & Li, B. (2024). *AI Risk Categorization Decoded (AIR 2024): From Government Regulations to Corporate Policies*.

AUTHOR BIOGRAPHY

Alexander B. Kinney, Ph.D., is an Assistant Professor in the Department of Sociology at Oberlin College. His research unpacks the dynamics of social control in gray markets, uses automated text modeling algorithms to study the logics of deviant behavior, and theorizes punishment in a cross-historical context. Recently, his work has been published in Social Problems, Crime & Delinquency, and Law & Policy, among other journals.

INSTITUTE FOR HOMELAND SECURITY

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Healthcare, Water/Wastewater and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University

Kinney, Alexander (2026). Regulating Artificial Intelligence in the State of Texas: Challenges and Opportunities. (Report No. 2026 - 1037). The Sam Houston State University Institute for Homeland Security.

Sam Houston State University™