1411 K Street N.W.
Suite 900
Washington, D.C. 20005
202-525-5717

Free Markets. Real Solutions.
www.rstreet.org

October 27, 2025

Office of Science and Technology Policy
2415 Eisenhower Avenue
Alexandria, VA 22314

Re: Request for Information on Regulatory Reform on Artificial Intelligence, Federal Register Number 2025-18737
Submitted Electronically
This Document is Approved for Public Dissemination.

Comments of the R Street Institute in
Request for Information on Regulatory Reform on Artificial Intelligence

I. OVERVIEW OF R STREET'S COMMENTS

Thank you for the opportunity to respond to the Request for Information on Regulatory Reform on Artificial Intelligence.

As a nonpartisan, nonprofit public policy research organization headquartered in Washington, D.C., the R Street Institute (RSI) appreciates the thoughtful steps the current administration has taken to secure America's position of global AI leadership. President Trump's Executive Order 14179, which rescinds the Biden administration's Executive Order 14110, signals a welcome return to a more open regulatory environment and pro-innovation policies that will enable the United States to maintain its competitive edge in artificial intelligence (AI) development.[1] This approach builds on President Trump's first-term AI initiatives, particularly Executive Order 13859, which committed federal resources to AI research and development, established AI

[1] "Executive Order on Removing Barriers to American Leadership in Artificial Intelligence," The White House, Jan. 23, 2025. https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence.

research institutes, and provided regulatory guidance to ensure AI remained an engine of U.S. economic and national security growth.[2]

We support the administration's focus on removing regulatory obstacles to AI innovation and its recognition that federal action is needed to eliminate barriers that prevent American companies from competing effectively on the global AI stage.

Over the past several years, RSI has brought together experts from academia, industry, civil society, and government to examine barriers to technological innovation across multiple domains. Our work has emphasized the need for regulatory frameworks that maintain legitimate safety, security, and consumer-protection objectives while facilitating—rather than hindering—innovation. This comment applies that framework to AI, identifying where federal regulations designed for pre-AI technologies create systematic barriers to AI development and deployment.

Although RSI generally prefers market-based solutions and state-level flexibility in regulatory policy, we recognize that certain reforms require federal action to prevent regulatory fragmentation that hinders interstate commerce and national competitiveness. Where we recommend federal frameworks or new guidance, we emphasize voluntary approaches, flexibility in implementation, and industry collaboration over prescriptive mandates.

In this spirit, we urge that those developing the AI Action Plan prioritize reforms in four key areas:

1. **Energy infrastructure.** Removing barriers to power generation and transmission that prevent AI data centers from accessing the reliable electricity they require, including streamlining interconnection processes, enabling co-located power arrangements, and expediting transmission development.
2. **Autonomous vehicles (AVs).** Modernizing federal motor vehicle safety standards (FMVSS) and commercial vehicle regulations to enable performance-based approaches rather than prescriptive requirements designed for human drivers.
3. **Cybersecurity.** Adapting federal cybersecurity frameworks to accommodate AI's continuous evolution, establishing AI-specific vulnerability disclosure processes, and streamlining export controls while strengthening agency capacity.
4. **Copyright law.** Ensuring that courts recognize AI training as transformative fair use, rejecting economically flawed "market dilution" theories and avoiding compulsory licensing regimes that would disadvantage American AI companies relative to international competitors.

[2] Executive Order on Maintaining American Leadership in Artificial Intelligence, Feb. 11, 2019. https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence.

II. ENERGY INFRASTRUCTURE: POWERING AI DEVELOPMENT

Our nation's ability to generate adequate energy to power advanced computational systems is key to maintaining America's AI superiority.[3] Many in the tech industry consider electric supply restrictions the largest barrier to domestic AI advancement.

AI data centers require extraordinary amounts of reliable electricity—often more than 500 megawatts per facility, roughly equivalent to the power needs of a medium-sized city.[4] Yet federal energy regulations designed for traditional power generation create significant barriers to reaching that level of production. Many of these limits stem from outdated policy rather than physical constraints; as a result, electricity restrictions are largely self-imposed, driving up costs and undermining reliability.[5] RSI research indicates that the primary problems with providing adequate, affordable, reliable power are rooted in regulatory barriers and monopoly utility structures.[6] These structural limitations suppress competition and innovation, reinforcing the need for stronger markets, not panicked interventions. This market-based approach aligns with the administration's broader goal of expanding domestic energy production and reliability.[7]

To meet this challenge, we must remove constraints across all forms of American energy. This includes constraints on the permitting and siting of nuclear, natural gas, and renewable energy power plants needed to meet market demands. It also includes similar constraints that inhibit the deployment of transmission lines connecting power plants to customers.

To address energy barriers, we recommend prioritizing three reforms: (1) removing barriers to energy-supplier choice for data-center developers, (2) completing generator-interconnection reform, and (3) streamlining permitting and siting of electric infrastructure.

1. Remove barriers to energy supplier choice for data center developers

Large energy consumers want the right to choose competitive energy suppliers that have developed faster, lower-cost, more innovative solutions for data centers than monopoly utilities have.[8] This requires removing discriminatory regulatory practices, such as restrictions

---

[3] Dorothy Mills-Gregg, "Interior Secretary Burgum: Energy growth is vital in 'AI arms race' with China," Inside AI Policy, Feb. 24, 2025. https://insideaipolicy.com/ai-daily-news/interior-secretary-burgum-energy-growth-vital-ai-arms-race-china.

[4] Devin Hartman and Olivia Manzagol, "AI's Energy Footprint Warrants Markets, Not Panic," R Street Institute, Sept. 26, 2024. https://www.rstreet.org/commentary/ais-energy-footprint-warrants-markets-not-panic.

[5] Ibid.

[6] Ibid.

[7] "Executive Order on Unleashing American Energy," The White House, Jan. 20, 2025. https://www.whitehouse.gov/presidential-actions/2025/01/unleashing-american-energy.

[8] Hartman and Manzagol, "AI's Energy Footprint Warrants Markets, Not Panic." https://www.rstreet.org/commentary/ais-energy-footprint-warrants-markets-not-panic.

on co-locating power plants and data centers, while ensuring that grid infrastructure costs are generally allocated to those who cause them.[9]

While RSI typically supports state flexibility in energy policy, a uniform federal framework for co-located arrangements is necessary to prevent state-by-state fragmentation that creates barriers to interstate energy markets and national AI infrastructure deployment. Congress should clarify federal jurisdiction over co-located generation and load arrangements when they involve interstate commerce or impact grid reliability. The Federal Energy Regulatory Commission (FERC) should establish clear, market-based frameworks that distinguish truly behind-the-meter operations from those meaningfully impacting the transmission system, with cost allocation reflecting actual grid usage rather than discriminatory treatment of specific industries. FERC should also apply its existing authority consistently to preempt state and local policies that discriminatorily target AI infrastructure relative to other large industrial consumers.

2. Finish generator interconnection reform

It typically takes as long as five years for new power plants to secure an agreement with grid operators to connect to the grid.[10] Over 2,600 gigawatts of generation capacity sits in FERC-jurisdictional interconnection queues—more than double the entire existing U.S. generation fleet.[11] In 2023, FERC took bipartisan steps to address this issue with Order 2023; however, key reforms were left unfinished and require further action.[12]

FERC should develop expedited, market-based interconnection pathways for generation facilities serving AI infrastructure that maintain safety and reliability standards while dramatically reducing approval timelines for projects demonstrating technical and financial readiness. Moreover, Congress should provide FERC with clear authority and direction to prioritize critical AI infrastructure in interconnection processes when existing authorities prove insufficient.

---

[9] Testimony of Kent Chandler, Federal Energy Regulatory Commission, "Commissioner-led Technical Conference Regarding Large Loads Co-located at Generating Facilities," 118th Congress, Nov. 1, 2024. https://www.rstreet.org/outreach/r-street-testimony-on-co-location-of-large-loads-with-generation.

[10] Joseph Rand et al., "Queued Up: Characteristics of Power Plants Seeking Transmission Interconnection," Lawrence Berkeley National Laboratory, 2025. https://emp.lbl.gov/queues.

[11] Ibid.

[12] Devin Hartman and Beth Garza, "R Street Input to FERC's Generator Interconnection Workshop," Federal Energy Regulatory Commission: Generator Interconnection Workshop, May 6, 2024. https://www.rstreet.org/outreach/r-street-input-to-fercs-generator-interconnection-workshop.

3. Streamline permitting and siting of electric infrastructure

Streamlining permitting and siting processes is essential to reduce litigation risk, provide better project information to state authorities, and refine federal backstop authority for interstate pipelines and transmission approvals.[13]

These reforms will ensure that data centers can access affordable and reliable power in the near term. In the long term, it is also important to ensure that the United States takes the lead in next-generation technologies like advanced nuclear, carbon capture, and energy storage. Improving the transparency, accountability, and performance of Department of Energy research and early deployment programs would drive innovation and put taxpayer dollars to better use.[14]

III. AUTONOMOUS VEHICLES: REMOVING REGULATORY BARRIERS

AVs represent one of AI's most significant near-term applications, having the potential to revolutionize transportation safety, efficiency, and accessibility. Yet federal motor vehicle safety standards (FMVSS) developed for human drivers create systemic barriers to AV deployment. Transportation Secretary Sean Duffy has expressed support for updating these standards to better accommodate AV technologies, creating an opportunity for meaningful reform.[15]

Current FMVSS establish uniform requirements for vehicle equipment like steering wheels, brake pedals, mirrors, dashboard warning lamps, and crash protection. Yet these requirements were all developed for human drivers; they fail to account for how AVs operate differently. As a result, the FMVSS block purpose-built robotaxis from being certified, force delivery AVs to unnecessarily comply with human-occupant standards, and create uncertainty about whether AV software updates require re-certification.

To address AV barriers, we recommend prioritizing three reforms: (1) enabling performance-based safety standards for AVs (2) establishing distinct regulatory frameworks for AV driving systems, and (3) developing AI-appropriate crash-investigation methodologies.

---

[13] Devin Hartman et al., "State and Local Permitting for the Energy Sector: Challenges and Opportunities," *R Street Policy Study* No. 313 (November 2024). https://www.rstreet.org/research/state-and-local-permitting-for-the-energy-sector-challenges-and-opportunities.

[14] Testimony of Devin Hartman, Subcommittee on Energy, House Committee on Energy and Commerce, "Hearing on Federal Energy Related Tax Policy and its Effects on Markets, Prices and Consumers," 115th Congress, March 29, 2017. https://docs.house.gov/meetings/IF/IF03/20170329/105798/HHRG-115-IF03-Wstate-HartmanD-20170329.pdf.

[15] "Trump's Transportation Secretary Sean P. Duffy Advances AV Framework with Plans to Modernize Safety Standards," National Highway Traffic Safety Administration. https://www.nhtsa.gov/press-releases/av-framework-plan-modernize-safety-standards.

1. Enable performance-based standards for AVs

The National Highway Traffic Safety Administration (NHTSA) should develop outcomes-based safety standards that focus on performance requirements rather than prescriptive equipment mandates. Instead of requiring specific physical controls designed for humans, standards should require demonstrated capability to perform driving functions safely (e.g., "maintain lane position within specified parameters" rather than "have steering wheel meeting specific dimensions"). This market-based approach would allow manufacturers to innovate ways to achieve safety objectives differently and perhaps more cost effectively.

Congress should provide NHTSA with greater flexibility for approving AVs that demonstrate equivalent or superior safety through alternative means. Current exemption authority under 49 U.S.C. § 30113 is capped at 2,500 vehicles per manufacturer annually—far too small for meaningful commercial deployment. Expanding this cap to at least 100,000 vehicles, extending authorization periods beyond five years, and setting a firm, six-month review timeline would allow scaled deployment while maintaining appropriate oversight.

2. Establish distinct frameworks for automated driving systems

Federal motor carrier regulations were written for human operators, imposing requirements such as hours-of-service limits, prohibitions on fatigued drivers, and commercial driver's licenses for individuals. This human-centric framework creates ambiguity about how AVs fit within existing rules.

Given the interstate nature of commercial trucking and the need for uniform national standards, Congress should establish distinct regulatory frameworks for automated driving systems that recognize AI as a fundamentally different class of operator category with distinct capabilities and limitations. This requires defining "automated driving system" as a distinct category, establishing system certification approaches (rather than individual licensing), and allocating liability clearly among manufacturers (for design defects), operators (for proper maintenance), and owners (for misuse).

The Federal Motor Carrier Safety Administration should develop flexible operational requirements for commercial AVs that focus on capability-based and condition-specific limitations rather than time-based rules designed around human fatigue, such as requiring systems to remain within certified operational design domains.

3. Develop AI-appropriate crash investigation methodologies

NHTSA's crash-reporting requirements lack frameworks for AI-specific investigation needs. Traditional investigations interview human drivers; AI systems require sensor log analysis, decision tree examination, and fleet-wide behavioral assessment.

NHTSA should develop voluntary guidance on investigation methodologies tailored to AI-driven vehicles, addressing data-logging requirements, decision-transparency needs, and comparative-analysis approaches. Guidance should clarify recommended logging practices (e.g., sensor inputs, detected objects, predicted trajectories, selected actions), establish evaluation

frameworks for assessing AI decisions, and specify procedures for protecting proprietary information while enabling meaningful safety oversight.

NHTSA should also work with industry to establish voluntary vulnerability tracking systems for AV driving systems that extend frameworks like the Common Vulnerabilities and Exposures (CVE) database used by the cybersecurity community to capture AI-specific security and safety issues when they emerge.

IV. CYBERSECURITY: SECURING AI SYSTEMS

Cybersecurity regulations designed for traditional information technology systems create barriers to AI deployment while failing to address AI-specific security challenges. As the administration works to modernize federal technology adoption, outdated cybersecurity frameworks prevent agencies from accessing cutting-edge commercial AI capabilities that could dramatically improve government efficiency and effectiveness.[16]

RSI research has demonstrated that AI security is not a constraint on innovation—it is a prerequisite for ensuring that America's AI advancements are scalable and resilient.[17] While adversaries may rush forward with fragile and opaque systems, America has a history of leading cutting-edge technological innovation by prioritizing secure, transparent technologies. Rather than constraining innovation, robust AI security provides the foundation for sustained American leadership.[18] The administration should review federal AI guidance, including the National Institute of Standards and Technology's (NIST's) AI Risk Management Framework (AI RMF 100-1), to ensure alignment with the AI Action Plan's principles of enabling innovation while maintaining appropriate security safeguards.

To address cybersecurity barriers, we recommend prioritizing three reforms: (1) modernizing FedRAMP for continuous AI evolution, (2) establishing AI vulnerability disclosure frameworks, and (3) advancing secure development practices for AI and machine learning (ML) systems.

1. Modernize FedRAMP for continuous AI evolution

FedRAMP's 6- to 18-month authorization process assumes that the systems it reviews are relatively static and can be assessed, approved, and operated in a linear fashion. Yet AI models retrain continuously (e.g., weekly, daily, constantly), creating a fundamental mismatching between static authorization cycles and dynamic system behavior. This mismatch increases

[16] Adam Thierer, "Trump's New AI Executive Order Begins Undoing Biden's Bureaucratic Mess," R Street Institute, Jan. 23, 2025. https://www.rstreet.org/commentary/trumps-new-ai-executive-order-begins-undoing-bidens-bureaucratic-mess.

[17] Haiman Wong, "Comments of the R Street Institute in Request for Information on the Development of a 2025 National AI R&D Strategic Plan," R Street Institute, May 22, 2025. https://www.rstreet.org/outreach/comments-of-the-r-street-institute-in-request-for-information-on-the-development-of-a-2025-national-artificial-intelligence-ai-research-and-development-rd-strategic-plan.

[18] Ibid.

authorization costs, prevents smaller AI firms from competing, and prevents agencies from receiving security patches that are immediately available to commercial users. RSI research has documented how the absence of universal, cross-sector AI security metrics creates inconsistencies in how organizations evaluate AI systems, leading to fragmented practices and potential blind spots in risk management.[19]

The Office of Management and Budget (OMB) and FedRAMP should develop flexible authorization approaches that accommodate AI's continuous evolution, focusing on assessing development processes and security practices rather than authorizing static system snapshots, with ongoing validation through automated monitoring. FedRAMP should establish AI-specific security guidance addressing model versioning, adversarial robustness, and training data integrity while allowing flexibility in implementation approaches. FedRAMP should also implement risk-based authorization timelines to enable faster access to lower-risk AI applications (30-90 days for routine productivity tools) while maintaining rigorous review for high-stakes deployments.

2. Establish AI vulnerability disclosure frameworks

The CVE system was designed for traditional software vulnerabilities (e.g., buffer overflows, SQL injection). AI systems face different vulnerability types: adversarial examples, prompt injection attacks, model poisoning, and model inversion.[20] No clear framework addresses what qualifies as an AI "vulnerability," how disclosure should occur, or whether researchers have legal protection when testing AI security under the Computer Fraud and Abuse Act.

RSI research has highlighted that adversarial nations are increasingly targeting open-source software and AI supply chains—including security tools, code repositories, model dependencies, training datasets, and compute infrastructure—introducing systemic vulnerabilities that bad actors can exploit to undermine U.S. national security.[21]

The Cybersecurity and Infrastructure Security Agency (CISA) should work with industry to develop voluntary frameworks for classifying and disclosing AI-specific vulnerabilities that account for unique AI characteristics. CISA should also facilitate coordinated disclosure processes that balance transparency with responsible remediation timelines, recognizing that addressing AI vulnerabilities may require model retraining rather than simple patches. Congress and the Department of Justice should clarify legal protections for good-faith AI security research to encourage responsible disclosure without risk of prosecution.

---

[19] Haiman Wong et al., "Assessing the Current State of AI-Cybersecurity Governance: Progress, Challenges, and Solutions," R Street Institute, May 21, 2024. https://www.rstreet.org/commentary/assessing-the-current-state-of-ai-cybersecurity-governance-progress-challenges-and-solutions.

[20] Haiman Wong et al., "Balancing Risk and Reward: AI Risk Tolerance in Cybersecurity," R Street Institute, April 15, 2024. https://www.rstreet.org/commentary/balancing-risk-and-reward-ai-risk-tolerance-in-cybersecurity.

[21] Haiman Wong, "DeepSeek's cybersecurity failures expose a bigger risk. Here's what we really should be watching," R Street Institute, Feb. 4, 2025. https://www.rstreet.org/commentary/deepseeks-cybersecurity-failures-expose-a-bigger-risk-heres-what-we-really-should-be-watching.

3. Develop secure development practices for AI/ML systems

OMB Memorandum M-22-18 requires federal agencies to obtain vendor attestations that software development conforms to NIST's Secure Software Development Framework (SSDF). SSDF addresses traditional software practices but not ML-specific needs like training data provenance, model versioning, distributed training security, adversarial robustness testing, and deployment monitoring.

NIST should establish voluntary guidance on secure development practices for AI/ML systems addressing unique considerations not captured by traditional frameworks, including data security throughout the AI lifecycle; model development and validation security; deployment security and monitoring; and AI supply chain security. This work should build on existing NIST guidance, including Secure Software Development Practices for Generative AI and Dual Use Foundation Models (SP 800-218A) and Cybersecurity Supply Chain Risk Management Practices (SP 800-161 Rev. 1).[22]

OMB should update federal AI procurement requirements to ensure that vendors demonstrate appropriate AI-specific security practices along with traditional software security measures, while maintaining flexibility for vendors to implement these practices in ways that suit their specific technologies and business models.

V. COPYRIGHT LAW: ENSURING AI TRAINING IS FAIR USE

Perhaps the most significant impediment to AI development is copyright law. Currently, more than 50 lawsuits against AI companies allege copyright infringement, with liability potentially running into the trillions.[23] Copyright litigation could significantly restrict the data needed to train frontier models, reducing AI's benefits and threatening American AI companies' global leadership. While other countries are considering text and data mining (TDM) exemptions for their AI industries, U.S. copyright law relies on the fair use doctrine to determine infringement.[24]

---

[22] Harold Booth et al., "Secure Software Development Practices for Generative AI and Dual Use Foundation Models," NIST SP 800-218A, July 2024. https://csrc.nist.gov/pubs/sp/800/218/a/final; Jon Boyens et al., "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations," NIST SP 800-161 Rev. 1, May 2022. https://csrc.nist.gov/pubs/sp/800/161/r1/upd1/final.

[23] "Master List, Copyright Lawsuits v. AI Companies in the U.S.," Chat GPT Is Eating the World, Sept. 16, 2025. https://chatgptiseatingtheworld.com/2024/08/27/master-list-of-lawsuits-v-ai-chatgpt-openai-microsoft-meta-midjourney-other-ai-cos; Shelly Palmer, "Damages: The AI Copyright Battle that Could Reshape the Industry," Aug. 13, 2025. https://shellypalmer.com/2025/08/seven-million-books-billions-in-damages-the-ai-copyright-battle-that-could-reshape-the-industry.

[24] "Issue Brief: Text and Data Mining and Fair Use in the United States," Association of Research Libraries, June 15, 2015. https://www.arl.org/news/fair-use-in-text-and-data-mining-arl-publishes-issue-brief.

The core issue is that training inputs for large language models (LLMs) are "quintessentially transformative" under fair use's first factor.[25] Training entails "fair learning"—extracting unprotected elements like syntax, style, and semantics, rather than copyrightable expression. This information is stored numerically in model parameters as weights and biases. LLMs transform information into knowledge rather than replicating original expressions.

Critically, the transformative act of training AI models (inputs) must not be conflated with products generated by AI models (outputs). These represent distinct legal questions. Training does not generate direct substitutes for original works, nor is copyrighted material visible in model parameters. The separate question of whether AI-generated outputs infringe is governed by existing copyright law frameworks. AI models are designed to avoid regurgitating copyrighted works, and developers actively work to prevent replication.[26] If outputs are found to infringe, existing law adequately addresses such concerns.

We recommend avoiding the following three harmful regulatory approaches: (1) reject "market dilution" as copyright harm, (2) avoid compulsory licensing regimes, and (3) maintain input/output distinction

1. Reject "market dilution" as copyright harm

The Copyright Office and others have advanced a theory that AI-generated content competing with human-created work represents copyright harm through "market dilution."[27] This theory is economically flawed. Market dilution constitutes a pecuniary externality—normal economic activity that only affects relative prices, such as when one company's better products reduce competitors' value. Copyright is not intended to protect creators from market competition, consumer preference changes, or technological advancement. The printing press, photography, sound recording, and digital distribution all disrupted creative markets. Accepting market dilution as copyright harm would fundamentally transform copyright's role while hampering valuable new technologies across all sectors.

2. Avoid compulsory licensing regimes

Some advocate for comprehensive licensing that would require payment for all works used to train AI models.[28] But compulsory licensing for all training data would not be desirable or practical at scale, given the massive datasets required for frontier models. This would create an administrative impossibility of tracking and compensating billions of training inputs. Licensing is

---

[25] *Bartz et al. v. Anthropic PBC*, 3:24-cv-05417 (N.D. Cal. 2024).

[26] Aakash Sharma, et al. *Nine Ways to Break Copyright Law and Why Our LLM Won't: A Fair Use Aligned Generation Framework*. (2025). 10.48550/arXiv.2505.23788.

[27] "Copyright and Artificial Intelligence Part 3: Generative AI Training (pre-publication version)," U.S. Copyright Office, May 2025. https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-3-Generative-AI-Training-Report-Pre-Publication-Version.pdf

[28] Copyright Alliance, "Position Paper: Artificial Intelligence," https://copyrightalliance.org/policy/positions/artificial-intelligence.

not a substitute for fair use—it is a mechanism for compensating uses that fall outside of fair-use boundaries. Voluntary licensing for high-value content is emerging organically in the market where it has become mutually beneficial.[29] But mandatory comprehensive schemes would impose untenable burdens and place American AI companies at a competitive disadvantage relative to countries providing TDM exemptions.

3. Maintain input/output distinction

Courts should recognize AI training as transformative fair use because it is extracting statistical patterns, not expressive content. The fair use doctrine has been interpreted with flexibility in the past (e.g., balancing technological developments and creator rights for earlier technologies like photocopiers, search engines, video recorders. It is sufficient to address AI without statutory changes. Courts should maintain the distinction between training inputs (transformative use) and generated outputs (evaluated for potential infringement of specific protected expression).

Courts should recognize AI training as transformative fair use under existing doctrine. Congress and agencies should reject market dilution as a basis for finding copyright harm, recognizing that competition from new technologies is normal economic activity rather than harm warranting regulatory intervention. Congress should decline to impose compulsory licensing regimes for AI training data, allowing voluntary market-based licensing to emerge where appropriate, while recognizing that fair use provides the appropriate framework for the vast majority of training activities. The Administration should advocate for fair use principles in international AI policy discussions, ensuring U.S. approaches maintain American competitiveness as other jurisdictions consider TDM exemptions.

AI diffusion will benefit myriad economic sectors beyond content industries, including healthcare, energy, climate change, finance, and telecommunications. Restricting AI training through narrow interpretations of fair use or licensing requirements would limit data for training frontier models, increase development costs (favoring large incumbents), fragment AI development globally, slow AI adoption across the economy, and potentially create trillions in liability exposure for existing systems.

VI. CONCLUSION

Federal regulations across energy infrastructure, AVs, cybersecurity, and copyright law create systemic barriers to AI innovation. The recommendations in this comment focus on outcomes-based reforms that maintain underlying policy objectives while enabling AI innovation by:

1. Modernizing authorization processes to accommodate AI's continuous evolution
2. Establishing clear frameworks that reduce regulatory uncertainty and enable investment

[29] See, e.g., Alexandra Bruell, "Amazon to Pay New York Times $20 Million a Year in AI Deal," *The Wall Street Journal*, July 30 2025 and "Meta in Major Talks with Publishers over AI Content Licensing," *The Decoder*, Sept. 18, 2025. https://the-decoder.com/meta-in-talks-with-major-publishers-over-ai-content-licensing.

3. Implementing risk-based approaches matching regulatory intensity to actual risks
4. Focusing on outcomes rather than prescriptive means
5. Maintaining proven legal principles that have successfully accommodated previous technological transitions

While RSI generally prefers market-based solutions and limited government intervention, certain reforms outlined here require federal action to prevent regulatory fragmentation, establish uniform standards for interstate commerce, and maintain American competitiveness in global AI development. Where new frameworks are recommended, we emphasize voluntary guidance, flexibility in implementation, and industry collaboration over prescriptive mandates.

American AI leadership requires regulatory frameworks that enable rapid innovation while maintaining appropriate safeguards. The reforms recommended herein would position the United States to lead AI development while ensuring safety, security, and appropriate protection of legitimate interests.

The Administration should work collaboratively with federal agencies to establish transparent timelines and accountability mechanisms for implementing the policy reforms outlined in this comment and the broader AI Action Plan. Clear milestones for regulatory reviews, voluntary guidance development, and framework updates would remove barriers to AI innovation while respecting agency expertise and stakeholder input. Regular public progress reporting would promote transparency and stakeholder engagement as agencies work to achieve the Administration's goal of American AI leadership.