FUTURE OF PRIVACY FORUM

CENTER FOR ARTIFICIAL INTELLIGENCE

March 14, 2025

Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue NW
Washington, DC 20504

VIA EMAIL: ostp-ai-rfi@nitrd.gov

RE: Comments from Future of Privacy Forum on the Development of an Artificial Intelligence (AI) Action Plan

Dear Office of Science and Technology Policy,

On behalf of the Future of Privacy Forum (FPF), we are writing in response to the Request for Information on the Development of an Artificial Intelligence (AI) Action Plan published in the Federal Register on February 6, 2025.[1] FPF is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies.[2]

We applaud the administration for seeking to develop a comprehensive national AI strategy. As recognized in President Trump's Executive Order 13859, "Maintaining American Leadership in Artificial Intelligence" (2019), the United States should be a

[1] 90 Fed. Reg. 9,088 (Feb. 6, 2025).
[2] The opinions expressed herein do not necessarily reflect the views of FPF's supporters or the Advisory Board.

global leader in driving technological breakthroughs and innovation in AI.[3] We completely agree that this should include the "development of appropriate technical standards" for AI testing and deployment, and that the United States must "foster public trust and confidence in AI technologies and protect civil liberties, privacy, and American values in their application in order to fully realize the potential of AI technologies for the American people."[4]

In order to accomplish these objectives, we recommend four key considerations:

1. A Federal Consumer Privacy Law Would Promote the Development of Innovative AI-Driven Products and Services, Establish Consistent Protections for Individuals, and Increase Regulatory Clarity for Businesses
2. Balanced Federal Preemption Would Set National Standards and Reduce Regulatory Burdens on US Companies
3. Promoting Industry-Led AI Standards and Interoperable Frameworks Would Advance American Leadership and Interests in Global AI Policy
4. Investing in R&D and Standards-setting for Privacy Enhancing Technologies (PETs) Would Benefit American Businesses Seeking to Balance Privacy and Utility in AI

1. A Federal Consumer Privacy Law Would Promote the Development of Innovative AI-Driven Products and Services, Establish Consistent Protections for Individuals, and Increase Regulatory Clarity for Businesses

In order to promote the development of AI-driven products and services while establishing consistent protections for individuals and also strengthening regulatory clarity for businesses, the administration should support Congress in drafting and passing a comprehensive baseline consumer privacy law. All of the traditional, historical safeguards of privacy law, which have been codified across many US sectoral laws for decades, are applicable to modern uses of AI that intersect with the use of personal data.

---

[3] Executive Order No. 13859, President Donald J. Trump, 84 Fed. Reg. 3,967 (Feb. 11, 2019). https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence.

[4] Executive Order No. 13859, President Donald J. Trump, 84 Fed. Reg. 3,967 (Feb. 11, 2019). These same principles are echoed in Executive Order 13960, President Donald J. Trump, 85 Fed. Reg. 78,939 (Dec. 3, 2020) and Office of Mgmt. & Budget, Exec. Office of the President, Dir. Russell T. Vought, OMB Memorandum M-21-06, Guidance for the Regulation of Artificial intelligence Applications (2020). https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government and https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf

In many cases, we are not convinced that it is always effective to broadly regulate the category of "artificial intelligence" per se, which is quickly becoming equivalent to "most technology." Yet there remains a significant underlying need for the United States to lead the world in our standards for the use of ***personal data*** - which impacts the overlapping concepts of privacy, data protection, cybersecurity, competitiveness, and individual autonomy and human flourishing.

Absent baseline federal protections for personal data, states have been actively filling the void by passing privacy laws that are now increasingly being viewed as vehicles to address policy concerns related to AI.[5] Other legal concepts, such as consumer protection law, product liability, negligence, and civil rights law, are also being applied to AI. While this approach brings promise of benefits to consumers, it also raises a real risk of a multiple-state divergence and overlapping regulatory overload for businesses in the answers to core legal questions, such as:

- Can first party data (e.g., on a social media platform) be re-purposed to train AI models without individual consent?
- What constitutes "de-identified" or "pseudonymized" data when training an AI system?
- What kind of fairness controls or transparency should be required for AI systems that are used to make important decisions that affect autonomy or human flourishing - such as a denial of medical insurance or treatment, a financial or lending decision, or a student's admission to (or rejection from) a college?
- What safeguards are appropriate for organizations that may use AI systems to evaluate or penalize workers rather than complement workers' productivity or achievements?[6]

---

[5] For example, several state Attorneys General recently published enforcement guidance on applying a range of state consumer protection, civil rights, and privacy laws to AI. *See, e.g.*, Guidance from Attorney General Ellen Rosenblum, "What you should know about how Oregon's laws may affect your company's use of Artificial Intelligence" (Dec. 24, 2024), *available at* https://www.doj.state.or.us/wp-content/uploads/2024/12/AI-Guidance-12-24-24.pdf.

[6] Workplace privacy is often exempted from proposals for comprehensive US privacy law for reasons of compliance or efficiency. However, FPF has urged policymakers to recognize the risks related to the use of AI to monitor workers or make employment decisions. This includes, for example, avoiding secrecy in use of AI monitoring tools, enabling sufficient human oversight and engagement, and exercising caution around the use of facial characterization and emotion inference technology. *See* Future of Privacy Forum, Best Practices for AI and Workplace Assessment Technologies (September 2023), https://fpf.org/resource/best-practices-for-ai-and-workplace-assessment-technologies/. These Best Practices align with Vice President J.D. Vance's stated principle at the 2025 Paris AI Action Summit that workers should be centered in national AI policy. *See* J.D. Vance, Remarks by the Vice President at the

These determine not only an organization's compliance obligations, but more fundamentally affect how AI-driven products and services are designed, trained, tested, and deployed, often long before they are launched in the market. Most such questions are not applicable to foundation model developers, but rather to the organizations that deploy those models in consumer-facing settings.

In some cases, the more data-restrictive principles of many privacy laws (e.g., data minimization, purpose limitation, and individual choice) will be at odds with important aspects of AI innovation and development, such as scraping publicly available data, or re-purposing first-party data for AI training. We recommend that a federal privacy law allow for sufficient flexibility to account for reconciling these kinds of potentially conflicting principles, including pragmatic mechanisms for clarifying or updating requirements in the future in light of rapidly changing technologies. Lawmakers might also consider incorporating limited carve-outs, exemptions, enforcement safe harbors, or regulatory sandboxes, to specifically promote development and innovation in AI.[7]

2. Balanced Federal Preemption Would Set National Standards, Reduce Regulatory Burdens on US Companies, and Support the US as a Global Leader

In crafting a federal law that would impact AI-driven products and services, one of the most complex challenges is federal preemption, or the extent to which the law will nullify the wide range of current and future state laws on the books.[8] Achieving the right balance of federal preemption with preservation of existing law would set strong, uniform national standards, reduce regulatory burdens on companies, and advance the United States as a global leader in AI policy. A federal privacy law must set nationwide, uniform rules for most collection and use of personal data; it must not simply become an additional framework that businesses must comply with.

As a starting point, a preemptive law for privacy and its related concepts that are relevant to AI - data protection, cybersecurity - would allow the United States to join most of the rest of the world in having strong uniform standards for the nation. In contrast to the current patchwork, in which states like California and Colorado are effectively shaping global policy, this would allow the US to advocate much more effectively that the

---

Artificial Intelligence Action Summit in Paris, France, The American Presidency Project, https://www.presidency.ucsb.edu/node/376290.

[7] *See* Datasphere Initiative, Sandboxes for AI: Tools for a New Frontier (Feb 2025), https://www.thedatasphere.org/datasphere-publish/sandboxes-for-ai/.

[8] *See* Stacey Gray, Future of Privacy Forum, Preemption in US Privacy Laws (June 2021), https://fpf.org/blog/preemption-in-us-federal-privacy-laws/ and Stacey Gray, Future of Privacy Forum, Navigating Federal Preemption through the Lens of Existing State Privacy Laws (July 2021), https://fpf.org/blog/navigating-preemption-through-the-lens-of-existing-state-privacy-laws/.

European Union and other jurisdictions consider conforming to, or converging with, the US's approach.

In particular, the preemption of "omnibus" state comprehensive privacy and AI laws with a strong federal framework would have the effect of significantly reducing regulatory burdens for US companies.[9] In the modern economy, most business practices involving personal data are inherently inter-state, especially as the scope of "personal data" has expanded – from traditional named records in the past, to modern processing of IP addresses, device identifiers, and other signals from connected products and services. This often makes it challenging if not impossible to operationalize differing local standards, or to retroactively conform AI development happening at a national or international scale to specific state requirements.

At the same time, policymakers should exercise caution in taking too heavy a hand with preemption in the context of "personal data" and especially "AI." This is because both terms - but especially "artificial intelligence" - will likely apply to many modern business technologies in some form. As a result, over-broad preemption poses the risks of:

- Creating blanket immunity from businesses' responsibilities under a wide range of existing law, such as product liability, negligence, civil rights, or contract law;
- Impacting hundreds of non-omnibus or niche privacy and AI-related protections passed by states over the years, such as laws related to library records, audio surveillance, AI-generated robo calls, or criminalization of non-consensual intimate imagery (e.g., deepfakes), which should not be overridden unless replaced by comparable protections at the federal level; and
- Disrupting several longstanding state privacy regimes regarding health records and financial data on which individuals have come to rely and in which companies have invested substantial compliance resources; it would be costly to disrupt these state laws.

Finally, it should be recognized that certain privacy and AI issues may always implicate local concerns in ways that should be reserved for state control when they impact the physical deployment or governance of technology, rather than the design or structure of data flows. For example, states should be permitted to decide whether to ban the use of facial recognition technology in retail or other public locations, or to require physical

[9] Approximately 20 states have passed "omnibus" privacy laws, or laws that regulate the collection and use of personal data across multiple sectors and industries under a single framework. In contrast, there are hundreds of targeted or niche state privacy laws on the books, governing library records, mugshots, anti-paparazzi, audio surveillance, digital assets, and more. *See* Stacey Gray, Future of Privacy Forum, *Navigating Federal Preemption through the Lens of Existing State Privacy Laws* (July 2021), https://fpf.org/blog/navigating-preemption-through-the-lens-of-existing-state-privacy-laws/.

signs disclosing such uses.[10] States and local bodies should also be encouraged to exercise oversight and control over the deployment of AI in traditionally local settings, such as in state government,[11] law enforcement, or education and classrooms.[12]

3. Promoting Industry-Led AI Standards and Interoperable Frameworks Would Advance American Leadership and Interests in Global AI Policy

The United States should continue to engage at the highest level with the global AI community, in order to advance American values in AI governance and shape the interoperable AI standards needed for US businesses to engage in responsible and innovative development, testing, and deployment at a national and international scale.[13] Much of this important work has been spearheaded by the US National Institute of Standards and Technology, including through their leadership in developing consensus Cybersecurity[14] and AI Risk Management[15] Frameworks.

As an example of global leadership, we support the United States continuing to re-envision and actively engage through organizations like the AI Safety Institute Consortium (AISIC) to develop standards and guidelines for AI red-teaming, evaluating capacity, and cybersecurity, among others. The United States and the United Kingdom were the first countries to establish AISIs,[16] leading to a growing network of AISIs around the world, such as in India, South Korea or Singapore, which have decided to cooperate within the International Framework of AI Safety Institutes.[17] Efforts such as these help

---

[10] Since 2021, New York City has required retail stores and other commercial establishments to post signs at entrances if they are collecting customers' biometric information. NYC Admin Code § 22-1202.
[11] A growing number of state executive branches have passed Executive Orders related to state government procurement and governance of AI. *See* Beth Do, *A Blueprint for the Future: White House and States Issue Guidelines on AI and Generative AI*, Future of Privacy Forum (Dec. 6, 2023), https://fpf.org/blog/a-blueprint-for-the-future-white-house-and-states-issue-guidelines-on-ai-and-generative-ai/.
[12] *See* Future of Privacy Forum Infographic, "Artificial Intelligence in Education: Key Concepts and Uses" (Feb 2025), https://fpf.org/blog/fpf-releases-infographic-highlighting-the-spectrum-of-ai-in-education/.
[13] National Institute for Standards and Technology, *A Plan for Global Engagement on AI Standards*, (July 26, 2024), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-5.pdf.
[14] US National Institute of Standards and Technology, *Cybersecurity Framework*, https://www.nist.gov/cyberframework (last visited Mar. 14, 2025).
[15] US National Institute of Standards and Technology, *AI Risk Management Framework*, https://airc.nist.gov/airmf-resources/airmf/ (last visited Mar. 14, 2025).
[16] Renan Araujo, *Understanding the First Wave of AI Safety Institutes: Characteristics, Functions, and Challenges*, Institute for AI Policy and Strategy (Oct. 7, 2024), https://www.iaps.ai/research/understanding-aisis#:~:text=In%20November%202023%2C%20the%20UK,with%20more%20likely%20to%20follow.
[17] Bethany Abbate, *Inaugural Convening of International Network of AI Safety Institutes Kicks Off In San Francisco*, Software Information Industry Association (Nov. 20, 2024),

ensure that US organizations lead and shape the development of international frameworks, and support American innovation and competitiveness by providing clear guidelines and standards for businesses.

The importance of industry-led global standards-setting aligns with the mandate from President Trump in Executive Order 13859 that American AI leadership requires "enhancing international and industry collaboration with foreign partners and allies."[18] It also aligns with the recent Bipartisan House Task Force Report on Artificial Intelligence, which states that "the strength of the United States in international standards development will be instrumental to its global technological leadership in the development and governance of artificial intelligence."[19] As the Report also notes, such standards-setting is often context-dependent, and the appropriate standards for things like de-identification of personal data may differ by sectoral application.

4. Investing in R&D and Standards-setting for Privacy Enhancing Technologies (PETs) Would Benefit American Businesses Seeking to Balance Privacy and Utility in AI.

The federal government should invest in R&D and standards-setting for privacy enhancing technologies (PETs) to provide businesses and the government the tools to unlock the utility of data in secure and privacy safe ways. Despite their importance, the widespread adoption of PETs such as homomorphic encryption, differential privacy, and federated learning,[20] often still remains hindered by limited computational resources and lack of regulatory clarity.[21]

However, PETs are increasingly critical in the design, development, training of AI systems to ensure legal compliance and minimize risk. They are also crucial technologies that can safeguard Americans' data from foreign adversaries while enabling cutting edge AI tools.

---

https://www.siia.net/inaugural-convening-of-international-network-of-ai-safety-institutes-kicks-off-in-san-francisco/.

[18] Executive Order No. 13859, President Donald J. Trump, 84 Fed. Reg. 3,967 (Feb. 11, 2019). https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence.

[19] 118th Congress, *Bipartisan House Task Force Report on Artificial Intelligence* (Dec 2024), *available at* https://obernolte.house.gov/AITFReport (page 66).

[20] For more resources on PETs, *see* Future of Privacy Forum's Repository for Privacy Enhancing Technologies, https://fpf.org/global/repository-for-privacy-enhancing-technologies-pets/.

[21] A lack of regulatory certainty is among the most significant barriers to adoption of privacy-enhancing technologies (PETs). *See* Future of Privacy Forum and Privacy Tech Alliance, *Privacy Tech's Third Generation: A Review of the Emerging Privacy Tech Sector* (June 2021), *available at* https://fpf.org/blog/new-fpf-report-highlights-privacy-tech-sector-evolving-from-compliance-tools-to-platforms-for-risk-management-and-data-utilization/.

American companies and researchers have been leaders in developing these technologies, and in particular, the National Institute of Standards and Technology has advanced American interests in standardizing their application.[22] Continuing to advance these efforts is critical to supporting the United States' AI competitiveness and leadership.

We welcome further engagement on this important topic.

Sincerely,

Stacey Gray, *Senior Director for Artificial Intelligence, FPF Center for Artificial Intelligence, Future of Privacy Forum*

Dr. Gabriela Zanfir-Fortuna, *Vice President for Global Privacy, Future of Privacy Forum*

This document is approved for public dissemination. The document contains no business-proprietary or confidential information. Document contents may be reused by the government in developing the AI Action Plan and associated documents without attribution.

[22] *See, e.g.*, NIST SP 800-226, *Guidelines for Evaluating Differential Privacy Guarantees* (March 2025), *available at* https://csrc.nist.gov/pubs/sp/800/226/final.