1411 K Street NW
Washington, D.C. 20005
202-525-5717

Free Markets. Real Solutions.
www.rstreet.org

March 20, 2024

National Telecommunications and Information Administration

1401 Constitution Ave. NW

Washington, D.C. 20230

Re: NTIA Docket No. 240216-0052 - "Openness in AI Request for Comment"

Thank you for providing the R Street Institute (R Street) with the opportunity to comment in response to the National Telecommunications and Information Administration's (NTIA) "Openness in AI Request for Comment" (*Request for Comment)* proceeding.[1] R Street is a nonprofit, nonpartisan public policy research organization. My name is Adam Thierer, and I am a senior fellow with R Street's Technology and Innovation Policy team. I also served as a commissioner on the U.S. Chamber of Commerce "Commission on Artificial Intelligence Competitiveness, Inclusion, and Innovation," which produced a major report on artificial intelligence (AI) policy issues.[2]

---

[1] National Telecommunications and Information Administration, "Dual Use Foundation Artificial Intelligence Models with Widely Available Model Weights," Docket Number 240216-0052, Feb. 21, 2024. https://www.ntia.gov/federal-register-notice/2024/dual-use-foundation-artificial-intelligence-models-widely-available.

[2] "Artificial Intelligence Commission Report," U.S. Chamber of Commerce, March 9, 2023. https://www.uschamber.com/technology/artificial-intelligence-commission-report.

R Street has published several essays relevant to this proceeding, including reports on "Flexible, Pro-Innovation Governance Strategies for Artificial Intelligence" and "Existential Risks and Global Governance Issues around AI and Robotics."[3]

This *Request for Comment* raises important issues about the future of algorithmic innovation in the United States. The most important thing to understand about open foundation models, and open-source AI technologies more generally, is that they are general-purpose technologies that are truly global in nature. By extension, these technologies and systems have important ramifications for the global competitiveness and geopolitical standing of nations.[4]

This is why public policy focused on algorithmic technologies—especially open AI systems—must be established with great care and flexibility. We strongly recommend the agency ensure that open-source AI systems are allowed to continue to develop without arbitrary limitations on their capabilities. Instead, our focus should be on how to maximize their benefits while addressing risks in the most flexible fashion possible using iterative standards and multistakeholder processes.[5] The agency already possesses the tools and methods needed to achieve that goal.

It is worth noting a potential contradiction that lies at the heart of the debate over open AI systems and the tension between this and previous NTIA proceedings. In discussions about the safety and effectiveness

---

[3] Adam Thierer, "Flexible, Pro-Innovation Governance Strategies for Artificial Intelligence," *R Street Policy Study* No. 283, April 2023. https://www.rstreet.org/research/flexible-pro-innovation-governance-strategies-for-artificial-intelligence; Adam Thierer, "Existential Risks and Global Governance Issues around AI and Robotics," *R Street Policy Study* No. 291, June 2023. https://www.rstreet.org/research/existential-risks-and-global-governance-issues-around-ai-and-robotics.

[4] Eric Schmidt, "Innovation Power: Why Technology Will Define the Future of Geopolitics," *Foreign Affairs* (March/April 2023). https://www.foreignaffairs.com/united-states/eric-schmidt-innovation-power-technology-geopolitics.

[5] Adam Thierer, "Statement for the Record on 'Artificial Intelligence: Risks and Opportunities,'" U.S. Senate Homeland Security and Governmental Affairs Committee, March 8, 2023. https://www.rstreet.org/outreach/testimony-on-artificial-intelligence-risks-and-opportunities.

of AI models, many academics and policymakers worry about the lack of transparency or "explainability" of proprietary algorithmic systems, especially of the largest models being created by major technology companies.[6] In fact, the NTIA has been considering questions about how to make AI systems more transparent as part of its "AI Accountability Policy" proceeding, which the agency launched last April.[7] Ironically, with this latest *Request for Comment*, the NTIA raises the opposite concern: whether open source systems might actually be too transparent and widely available.

What is perhaps overlooked is that we have a range of constantly expanding options along the "open vs. closed" continuum of software and hardware systems, including new AI models. The NTIA notes that "'openness' or 'wide availability' of model weights are also terms without clear definition or consensus" and the agency speaks of the "gradients" of openness.[8] This is correct, but it is important to understand that no formula exists whereby policymakers can get things "just right" when it comes to determining the optimal amount of openness or transparency of algorithmic systems. It would be a mistake for government to unnaturally tip the balance in either direction when the optimal amount of model openness or transparency is unclear. There is great benefit in allowing both open and closed systems to evolve organically over time because there are unique benefits to AI systems along that spectrum of options. Thus, *the proper policy position for government toward open vs. closed systems should be one of technological agnosticism, and policymakers should not look to artificially tip the scales in either direction*.

---

6 Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press, 2016).

7 National Telecommunications and Information Administration, "AI Accountability Policy Request for Comment," United States Department of Commerce, Docket No. 230407-0093, RIN 0660-XC057, April 11, 2023. https://www.ntia.gov/issues/artificial-intelligence/request-for-comments.

8 National Telecommunications and Information Administration, p. 6.

With this proceeding, the agency must avoid doing that by imposing too great a burden on open AI systems.

I. Open systems offer clear benefits, which could easily be lost if overregulated

Open-source systems have had a long and important history in the digital technology ecosystem because they are built on the accumulated knowledge and efforts of developers cooperating across the world.[9] A recent National Institute of Standards and Technology (NIST) report explained how open source "has established itself as an indispensable methodology for developing software," and it explored the many benefits of open-source technologies, including how those capabilities are now being used in more advanced AI systems.[10] The agency highlighted the benefits of open systems in terms of "democratizing access, leveling the playing field, enabling reproducibility of scientific results," and other positive attributes.[11] Similarly, a recent Stanford University report explained how open AI systems have the benefit of "distributing power, catalyzing innovation, and ensuring transparency."[12] Other experts have likewise argued that open-source technologies "are the bedrock for grassroots innovation in AI" and can help "promote a diverse AI ecosystem."[13] Finally, open-source AI systems can be rapidly modified for more widespread, multilingual, and highly tailored uses to meet the needs of various

---

[9] Alice Ivey, "The importance of open-source in computer science and software development," *Cointelegraph*, Feb. 9, 2023. https://cointelegraph.com/news/the-importance-of-open-source-in-computer-science-and-software-development.

[10] Apostol Vassilev et al., "Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations," NIST Trustworthy and Responsible AI, NIST AI 100-2e2023 (January 2024), p. 53. https://doi.org/10.6028/NIST.AI.100-2e2023.

[11] Ibid.

[12] Rishi Bommasani et al., "Considerations for Governing Open Foundation Models," Stanford University Human-Centered Artificial Intelligence, December 2023, p. 4. https://hai.stanford.edu/sites/default/files/2023-12/Governing-Open-Foundation-Models.pdf.

[13] Ben Brooks, "Open-Source AI Is Good for Us," *IEEE Spectrum*, Feb. 8, 2024. https://spectrum.ieee.org/open-source-ai-good.

people and groups across the globe.[14] Two security experts noted that new open-source models "are much more accessible and easier to experiment with," and "can now be customized on a mid-priced laptop in a few hours." The experts concluded that "[t]his fosters rapid innovation."[15]

Despite these clear benefits, fears of misuse tend to drive the debate over open AI systems today, including concerns about how they might be used to build dangerous weapons or create misinformation campaigns.[16] While these risks deserve to be taken seriously, it is vital for the agency to keep two facts in mind. First, many of the supposed risks of open AI systems are shared with many other "open" information mediums and technologies. Descriptions about how to build dangerous weapons have appeared in books, magazines, blog posts, and online videos. Likewise, "misinformation," however defined, is a problem that goes back to the rise of the printing press.[17] Setting aside the thorny issue of whether it is constitutionally permissible under the First Amendment for the government to regulate speech about the creation of dangerous weapons or misinformation, the fact is that these concerns have long existed in various contexts. Open-source AI models could exacerbate those risks, but it might also provide a path to addressing many of these concerns.

Second, the risks of open systems must be weighed carefully against the equally serious danger that overregulation could undermine their vibrancy (or even their very existence), thus giving rise to different

---

[14] Kai-Fu Lee, "Artificial Intelligence Needs Open-Source Models to Reach Its Potential," *Wall Street Journal*, Nov. 29, 2023. https://www.wsj.com/articles/artificial-intelligence-needs-open-source-models-to-reach-its-potential-e1f47d3f.

[15] Bruce Schneier and Jim Waldo, "Big Tech Isn't Prepared for A.I.'s Next Chapter," *Slate*, May 30, 2023. https://slate.com/technology/2023/05/ai-regulation-open-source-meta.html.

[16] David Evan Harris, "Open-Source AI Is Uniquely Dangerous," *IEEE Spectrum*, Jan. 12, 2024. https://spectrum.ieee.org/open-source-ai-2666932122.

[17] Julie Posetti and Alice Matthews, "A Short Guide to the History of 'Fake News' and Disinformation: A New ICFJ Learning Module," International Center for Journalists, July 23, 2018. https://www.icfj.org/news/short-guide-history-fake-news-and-disinformation-new-icfj-learning-module; Jacob Soll, "The Long and Brutal History of Fake News," *Politico Magazine*, Dec. 18, 2016. https://www.politico.com/magazine/story/2016/12/fake-news-history-long-violent-214535.

dangers. As one open source developer noted, if heavy-handed compliance mandates are imposed on open-source systems, "[d]evelopers operating from dorm rooms and dining tables won't be able to comply with the premarket licensing and approval requirements that have been proposed" because of their smaller size.[18] "Grassroots innovation may become collateral damage," he argued, because "regulations could put the brakes on this culture of open development in AI."[19] Other researchers agree. "The effects of these regulations may turn out to be impossible to undo, and therefore we should be extremely careful before we legislate them," argued the founding researcher at Fast.AI, a nonprofit research group focused on democratizing AI development and use.[20] He worries that overregulation of open-source systems could "ultimately lead to the frontier of AI becoming inaccessible to everyone who doesn't work at a small number of companies, whose dominance will be enshrined by virtue of these ideas. This is an immensely dangerous and brittle path for society to go down."[21]

This is why it would be a serious mistake for government to impose arbitrary limitations on the power of open-source algorithmic systems. Again, these are truly global general-purpose technologies. Digital technology developers respond to the signals that national policymakers send when they craft laws and regulations for emerging information and computational technologies. We increasingly live in a world characterized by "global innovation arbitrage," in which developers and investors often move their talent and resources to wherever they are treated most hospitably.[22] This means that domestic policy decisions that discourage innovation and investment in next-generation algorithmic and computational

---

[18] Brooks. https://spectrum.ieee.org/open-source-ai-good.

[19] Ibid.

[20] Jeremy Howard, "AI Safety and the Age of Dislightenment," Fast.AI, July 10, 2023. https://www.fast.ai/posts/2023-11-07-dislightenment.html.

[21] Ibid.

[22] James Pethokoukis, "Global Innovation Arbitrage and Driverless Cars," American Enterprise Institute, Aug. 23, 2016. https://www.aei.org/economics/global-innovation-arbitrage-and-driverless-cars.

capabilities can result in a net loss of competitive advantage for nations because, as two leading software security experts noted, "there are simply too many researchers doing too many different things in too many different countries."[23]

II. The most important AI safety consideration of all

A loss of competitive advantage in advanced computation through burdensome regulatory policies could have broader implications for U.S. geopolitics and national security. There is a symbiotic relationship between the strength of a nation's technology base and its ability to address various threats to its security.[24]

This explains why this proceeding is framed improperly. While it is sensible to evaluate the safety of open AI models, *the greatest danger of all would be the absence of these technological capabilities within our own nation*. Policymakers must allow powerful open-source AI systems to be developed domestically to ensure both that the United States stays ahead of potential adversaries on this front and also to ensure we learn collectively how to better address the risks and misuses of these technologies in a real-time fashion.

This principle is especially important when considering the growth of China's computational capabilities, including those in the field of open-source systems.[25] As analysts with the Mercator Institute for China Studies have noted, China is a country "often seen as discouraging decentralized forms of innovation,"

---

[23] Schneier and Waldo. https://slate.com/technology/2023/05/ai-regulation-open-source-meta.html.

[24] Loren B. Thompson, "Why U.S. National Security Requires A Robust, Innovative Technology Sector," Lexington Institute, Oct. 8, 2020. https://www.lexingtoninstitute.org/why-u-s-national-security-requires-a-robust-innovative-technology-sector.

[25] Rebecca Arcesati and Caroline Meinhardt, "China's Open-Source Tech Development: Insights into a growing ecosystem," Mercator Institute for China Studies, May 2021. https://merics.org/sites/default/files/2021-05/MERICS%20Primer%20Open%20Source%202021_0.pdf.

but is now "bolstering the development of a vibrant open-source ecosystem."[26] China's Ministry of Industry and Information Technology has been actively seeking to bolster the development of open-source projects that can counter other global systems, most of which originated in the United States.[27] Recent Chinese open-source AI startups have grown more sophisticated and now rival leading American models.[28] Upon launch late last year, Chinese startup 01.AI received a $1 billion valuation, leading *Wired* to declare that "This Chinese Startup is Winning the Open Source AI Race."[29]

It would be a mistake to believe that China is the only serious competitor in terms of advanced computational capabilities, however. The recent effort to develop the world's largest open-source foundation model illustrates how there is intense competition to U.S. developers coming from numerous countries. On July 18, 2023, U.S.-based Meta announced it was launching its 70-billion parameter "Large Language Model Meta AI" (LLaMA 2) for open source commercial use and research.[30] This was an important moment for open-source AI because it represented the release of the biggest open-source model yet, and one that rivalled many of the leading proprietary foundation models from other players, such as OpenAI.[31] But Meta also faces stiff competition from other open-source platforms, such as Falcon. Falcon is a large-scale open-source AI model that is royalty-free for research

---

[26] Rebecca Arcesati and Caroline Meinhardt, "China bets on open-source technologies to boost domestic innovation," Mercator Institute for China Studies, May 19, 2021. https://merics.org/en/report/china-bets-open-source-technologies-boost-domestic-innovation.

[27] Ibid.

[28] Jose Antonio Lanz, "New Open Source AI Model from China Boasts Twice the Capacity of ChatGPT," *Emerge*, Nov. 15, 2023. https://decrypt.co/206195/new-open-source-ai-model-from-china-boasts-twice-the-capacity-of-chatgpt.

[29] "Chinese AI startup 01.AI valued at more than $1bn," *Verdict*, Nov. 6, 2024. https://www.verdict.co.uk/01-ai-valued-at-over-1bn; Will Knight, "This Chinese Startup Is Winning the Open Source AI Race," *Wired*, Jan. 23, 2024. https://www.wired.com/story/chinese-startup-01-ai-is-winning-the-open-source-ai-race.

[30] "Meta and Microsoft Introduce the Next Generation of Llama," Meta, July 18, 2023. https://about.fb.com/news/2023/07/llama-2.

[31] Savannah Fortis, "Meta is building an AI model to rival OpenAI's most powerful system," *Cointelegraph*, Sept. 11, 2023. https://cointelegraph.com/news/meta-building-ai-model-rivals-open-ai.

or commercial use, and it has become an important platform that other developers around the world have used to build bespoke open models of their own. Falcon was created by the Abu Dhabi-based Technology Innovation Institute (TII), a research center supported by the government of the United Arab Emirates and its Advanced Technology Research Council.[32]

On Sept. 6, 2023, less than two months after Meta launched its record-breaking open-source model, the TII introduced Falcon 180B, a 180-billion parameter open AI model that was 2.5 times larger than Meta's LLaMa.[33] In other words, America's supremacy in open-source foundation models lasted less than two months—at least based on the largest model on the market currently as measured in parameters. While the open-source ecosystem in the United States remains quite vibrant, this was an astonishing development that should serve as a wake-up call for America policymakers: U.S. innovators face stiff global competition for open-source AI and all large AI models.

To be clear, the United Arab Emirates is not an adversary of the United States, and we need not panic simply because some nations are developing advanced computational capabilities—open sourced or otherwise. But the power of Falcon, and the speed with which it was developed, should also not be taken lightly. As has been the case in China, the government of the United Arab Emirates has invested massive resources into its nation's computational capabilities. Nothing U.S. policymakers say and do to regulate open-source systems in the United States will limit what foreign leaders or innovators in other countries do to advance their own computational capabilities. The most dangerous myth in the field of AI policy is that American policy preferences can dictate global outcomes. The U.S. government does have

---

[32] "About TII," Technology Innovation Institute, last accessed March 4, 2024. https://www.tii.ae/about-us.

[33] "Technology Innovation Institute Introduces World's Most Powerful Open LLM: Falcon 180B," Technology Innovation Institute, Sept. 6, 2023. https://www.tii.ae/news/technology-innovation-institute-introduces-worlds-most-powerful-open-llm-falcon-180b.

considerable leverage with some nations, and can work with other nation-states to lean on other nations to limit or alter their own policies and development patterns. But barring extreme steps that would give rise to grave geopolitical risks (such as armed interventions), there is no way for the United States to set AI policy for the world.[34] Correspondingly, any domestic restriction that binds U.S. AI developers but not computational development by potential adversaries could undermine our nation's innovative potential and security.

III. Pragmatic steps toward AI safety

That being said, U.S. policymakers can continue to work with developers of advanced algorithmic systems to advance safety in a collaborative, flexible, bottom-up fashion. As has been the case throughout the internet's history, *multistakeholderism* and *iterative standards* will continue to play an essential role in advancing safety and security outcomes, including for open AI systems.

From the outset of the digital revolution, engineers and developers relied upon the notion of "running code and rough consensus" as a pragmatic governance philosophy of continuous digital technology iteration and improvement, and it has been particularly important for open-source systems.[35] Online innovation has never been governed by a static set of rules but instead by a constantly evolving set of best practices, norms, and standards. Laws and regulations have operated as a backstop to address thornier problems that develop, but only after other approaches have been exhausted. This trial-and-error approach to technological governance is what made the United States the global leader in digital

[34] Thierer, "Existential Risks and Global Governance Issues," p. 30. https://www.rstreet.org/research/existential-risks-and-global-governance-issues-around-ai-and-robotics.

[35] Ibid, p 24.

technology over the past quarter century, and it is essential this model be preserved if the nation is going to continue to be a leader in AI and advanced computation.

This same notion of "running code and rough consensus" can help shape better outcomes for open-source AI systems through the development of safety standards and security practices that are refined in a flexible, voluntary way to adapt to new circumstances and concerns. Luckily, this process is already well underway through the development of various ethical codes, security and safety best practices, and information-sharing standards developed by industry groups, technical bodies, government agencies, and various researchers. A recent R Street report assessed many of those efforts and discussed how they were rooted in a common set of best practices and principles.[36]

These same standards and principles are being applied to open-source systems already. In a recent major study on open AI systems, researchers from Carnegie Mellon University and Intel Labs identified six possible principles and best practices that can help improve open-source safety outcomes.[37] They include:

1. Take a stand on unethical uses, and enforce it.
2. Educate on project-specific harms.
3. Consider technical restrictions on use.
4. Leverage reputational incentives.
5. Platforms should publish and consistently enforce policies that consider downstream uses.
6. Publicize and study Ethical Source licenses.

---

[36] Thierer, "Flexible, Pro-Innovation Governance Strategies for Artificial Intelligence," p. 11. https://www.rstreet.org/research/flexible-pro-innovation-governance-strategies-for-artificial-intelligence.

[37] David Gray Widder et al., "Limits and Possibilities for 'Ethical AI' in Open Source: A Study of Deepfakes," *FAccT '22* (June 20, 2022), pp. 2035-2046. https://dl.acm.org/doi/abs/10.1145/3531146.3533779.

These are sensible guidelines, and many of these same ideas were echoed by a new report from 25 leading researchers on open AI systems, who recommend that AI developers strive to constantly identify and refine "the responsible AI practices they implement and the responsible AI practices they recommend or delegate to downstream developers or deployers." [38] Due to the "significant uncertainty for several misuse vectors due to incomplete or unsatisfactory evidence," they note that only constant vigilance by developers and researchers can adequately address constantly evolving threat landscape.[39]

These recommendations are rooted in two general commonsense principles. First, *safety is an ongoing journey, not a final destination*. There are no silver-bullet solutions to any of the potential risks associated with advanced algorithmic systems. Open systems can certainly create risks, and many unexpected new issues will develop over time, but that is why it is essential to keep dialogue and research open and ongoing. Importantly, there are many security benefits associated with AI systems that can facilitate real-time threat detection and correction.[40] By their very nature, open systems help us find vulnerabilities and quickly address them. Regulation could short-circuit that corrective process of trial-and-error learning, leading to different safety and security vulnerabilities.

Second, *AI policy should focus primarily on bad outputs and bad actors, not on the underlying process by which algorithmic systems operate*.[41] AI governance strategies should not overregulate the underlying model or platform in an attempt to preemptively head-off every hypothetical worst-case scenario because

---

[38] Sayash Kapoor et al., "On the Societal Impact of Open Foundation Models," The Center for Research on Foundation Models, Feb. 27, 2024. p. 8. https://crfm.stanford.edu/open-fms/paper.pdf.

[39] Ibid.

[40] Haiman Wong et al., "Harnessing AI's Potential – Identifying Security Risks to AI Systems," R Street Institute, Feb. 21, 2024. https://www.rstreet.org/commentary/harnessing-ais-potential-identifying-security-risks-to-ai-systems.

[41] Jay Obernolte, "The Role of Congress in Regulating Artificial Intelligence," *The Ripon Forum* 57:3 (June 2023). https://riponsociety.org/article/the-role-of-congress-in-regulating-artificial-intelligence.

that would undermine the innovative potential of the open source AI more generally. As the Fast.AI founding research noted, "because we are discussing general-purpose models, we *cannot* ensure safety of the model itself — it's only possible to try to secure the *use* of a model."[42] Of course, researchers have noted that there will also be significant challenges with constraining downstream uses of open AI technologies once they are released.[43] Nonetheless, the proper locus of AI policy lies with a more targeted, risk-based approach that zeroes in on specific uses and users that raise serious safety and security concerns.[44] This use-focused approach will not disrupt the vibrancy of the broader open source ecosystem.

IV. The crucial importance of ongoing multistakeholder processes

Policymakers can help facilitate the development and adoption of such best practices over time by once again relying on multistakeholder processes to address problems in a more flexible, agile, and iterative fashion. NIST has already made important strides in this regard with its various multistakeholder risk frameworks and evolving set of procedures for convening relevant parties, calling for constant input, and then issuing iterative reports highlighting areas of consensus.

NIST's *Artificial Intelligence Risk Management Framework 1.0* (*AI RMF*) is a voluntary, consensus-driven guidance process that has earned widespread support from distinct stakeholders.[45] The *AI RMF* builds on the ethical frameworks and best practices developed by many different organizations and is "designed to address new risks as they emerge" and help create more trustworthy AI systems over

---

[42] Howard. https://www.fast.ai/posts/2023-11-07-dislightenment.html.

[43] Widder et al., p. 9. https://dl.acm.org/doi/abs/10.1145/3531146.3533779.

[44] Adam Thierer, "The Most Important Principle for AI Regulation," R Street Institute, June 21, 2023. https://www.rstreet.org/commentary/the-most-important-principle-for-ai-regulation.

[45] National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, U.S. Department of Commerce, January 2023. https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf.

time.[46] "This flexibility is particularly important where impacts are not easily foreseeable and applications are evolving," the agency noted.[47] Importantly, the *AI RMF* builds on other NIST consensus-based multistakeholder frameworks, such as the NIST *Privacy Framework* and the recently updated NIST *Cybersecurity Framework 2.0*, which "does not prescribe how outcomes should be achieved," but instead provides "guidance on practices and controls that could be used to achieve those outcomes."[48]

These NIST frameworks have been multi-year efforts focused on building collaborative approaches to privacy and security across industry, academia, and government not only in the United States, but with others around the world. The most innovative thing about these frameworks is the way they are versioned like software, reflecting the way that digital technology governance needs to be highly agile and iterative, responding to the way technology itself evolves at an increasingly rapid pace. This represents a smart move away from the more rigid regulatory approaches of the past, which established static policies that were often left unchanged for years or longer. AI policy must work differently, and the NIST frameworks give us a constructive path forward. The formation of NIST's new AI Safety Institute also provides another mechanism for coordinating governance best practices for algorithmic systems.[49] It serves as a way for government to help "institutionalize frontier AI safety," as many academics have called for, without imposing burdensome mandates that might undermine algorithmic innovation and

---

[46] Ibid., p. 4.

[47] Ibid.

[48] National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0*, U.S. Department of Commerce, Feb. 26, 2024, p. i. https://doi.org/10.6028/NIST.CSWP.29.

[49] National Institute of Standards and Technology, "U.S. Commerce Secretary Gina Raimondo Announces Key Executive Leadership at U.S. AI Safety Institute," U.S. Department of Commerce, Feb. 9, 2024. https://www.nist.gov/news-events/news/2024/02/us-commerce-secretary-gina-raimondo-announces-key-executive-leadership-us.

competition, especially among open-source systems.[50] This process should provide a way to refine risk-analysis techniques for advanced AI systems and devise metrics for better measuring outcomes.

In addition to the important role that NIST has in this process, the NTIA also has a role to play. The NTIA has played a crucial part in facilitating ongoing multistakeholder "soft law" efforts in the past to address other technical matters where collaboration and coordination were needed.[51] "We believe that the multi-stakeholder approach, despite its challenges, works remarkably well at addressing emerging internet and technology policy questions," the former leaders of the Obama administration NTIA noted shortly after leaving office.[52] "We are just beginning to appreciate the full power and potential applicability of the approach," they concluded, because multistakeholderism represents "a process that is flexible and allows businesses to adjust in response to the rapid changes in their economic and technical environments."[53]

This is the path forward for overseeing open-source AI developments. Importantly, policymakers must not simply focus of the risks of algorithmic innovation, they must also identify the risks associated with over-regulation of algorithmic systems, which could be even more problematic. "Policymakers should also proactively assess the impacts of proposed regulation on developers of open foundation models" and understand that "some policy proposals impose high compliance burdens for these developers, and

---

[50] Markus Anderljung et. al., "Frontier AI Regulation: Managing Emerging Risks to Public Safety," *arXiv* 2307:03718 (Nov. 7, 2023) pp. 17-18. https://arxiv.org/abs/2307.03718.

[51] Adam D. Thierer, "Soft Law in U.S. ICT Sectors: Four Case Studies," *Jurimetrics* 61:1 (April 20, 2021), pp. 79-119. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3777490.

[52] Lawrence E. Strickling and Jonah Force Hill, "Multi-stakeholder internet governance: successes and opportunities," *Journal of Cyber Policy* 2:3 (Nov. 28, 2017), p. 310. https://www.tandfonline.com/doi/abs/10.1080/23738871.2017.1404619.

[53] Ibid.

such policies should only be pursued with sufficient justification of the adverse effect on the open foundation model ecosystem."[54]

Conclusion

In closing, we will reiterate some core principles that should guide this proceeding, most of which we listed in our previous submission to the agency in its AI Accountability Policy proceeding.

The agency should remember that America's unique advantage over other nations has been a flexible and adaptive approach to digital technology policy.[55] Digital innovation, especially open-source innovation, has blossomed because policy has allowed for a general freedom to innovate, and when challenges have arisen or dangers were discovered, we have used ongoing multistakeholder efforts and a variety of ex-post policy solutions to address those problems.[56] This agile governance approach helps provide the public more innovative options, but it also provides our nation a more secure technological base.[57] The agency should build on that model when formulating governance approaches for new computational systems and look to keep the United States at the forefront of the next great technological revolution.

Finally, history offers us some lessons in terms of the need for policy humility. There were many fears in the late 1990s about the rise of open-source systems, and for a time, the U.S. government also treated powerful computation and encryption as dangerous "munitions" that should be subjected to export

---

[54] Kapoor et al., p. 9. https://crfm.stanford.edu/open-fms/paper.pdf.

[55] Adam Thierer, *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom*, 2nd ed. (Mercatus Center at George Mason University, 2016).

[56] Ibid.

[57] Adam Thierer, "U.S. Chamber AI Commission Report Offers Constructive Path Forward," R Street Institute, March 9, 2023. https://www.rstreet.org/commentary/u-s-chamber-ai-commission-report-offers-constructive-path-forward.

controls.[58] Luckily, this moment passed and citizens today benefit greatly from open-source systems and encryption technologies. We need to exercise similar forbearance toward modern digital systems, especially open-source AI.

Respectfully submitted,

_____

Adam Thierer

Senior Fellow

R Street Institute

1411 K St. NW

Washington, D.C. 20005

athierer@rstreet.org

[58] Louis Anslow, "When the Mac was a 'munition,'" *Freethink*, Jan. 30, 2024. https://www.freethink.com/opinion/power-mac-g4.