Carl Szabo
Vice President & General Counsel, NetChoice
1401 K Street NW, Ste 502
Washington, DC 20005

NetChoice
Defending Free Speech and Free Enterprise Online

Docket No. 240119-0020
RIN 0694-AJ35

COMMENTS

April 22, 2024

Comment of NetChoice
Docket No. 240119-0020
RIN 0694-AJ35

Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities

Introduction

NetChoice appreciates the opportunity to comment on the Department of Commerce's notice of proposed rulemaking (NPRM) on addressing the national emergency with respect to significant malicious cyber-enabled activities.[1]

NetChoice is a trade association of leading e-commerce and online businesses who share the goal of promoting convenience, choice, and commerce on the internet.[2] Our mission is to make the internet safe for free enterprise and free expression. We work to promote the integrity and availability of the global internet and are significantly engaged in public policy issues impacting e-commerce.

While NetChoice supports the Administration's goal of protecting U.S. interests from foreign cyber threats, we are concerned that some NPRM provisions could stifle AI innovation, impose onerous requirements on U.S. infrastructure as a service (IaaS) providers, and dangerously increase government dependence on a single technology vendor. Our comments focus on four key areas:

1. Avoiding limitations on AI innovation and deployment: The U.S. AI leadership depends on rapid experimentation and iteration. The proposed technical conditions and reporting requirements for "large AI models" risk creating a chilling effect. We do not need an “FDA for AI.”[3]

[1] NPRM, Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities, Docket No. 240119-0020.
[2] About NetChoice, https://netchoice.org/about/.
[3] *See, e.g.*, Ryan Hagemann, Jennifer Huddleston Skees, and Adam Thierer, “*Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future*,” Colorado Technology Law Journal 17 (2018): 37–130, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3118539.

2. Leveraging existing laws to address AI risks: There are robust legal frameworks in place today to address potential AI harms, including in areas like privacy, security, consumer protection, and antidiscrimination.[4] Enforcing these existing laws should be the priority over premature AI-specific regulations.
3. Balancing costs and benefits of identity verification requirements: The proposed identity verification requirements for IaaS providers and foreign resellers are overly burdensome, not sufficiently targeted, and risk advantaging foreign competitors.[5] A more risk-based approach is needed.
4. Mitigating risks of overreliance on Microsoft: The government's dependence on Microsoft products raises serious concerns, as evidenced by the company's recent major security breaches.[6] Diversifying technology providers and using the government's leverage to drive security improvements at Microsoft are essential.

I. Avoiding Limitations on AI Innovation

The NPRM proposes requiring U.S. IaaS providers to report when foreign persons use their services to train “large AI models” with "potential capabilities that could be used in malicious cyber-enabled activity," based on technical conditions set by the Secretary.[7]

This risks severely constraining AI development, which depends on rapid testing of new model architectures, training techniques, datasets, and applications.[8] Establishing upfront technical criteria or a de facto approval process for “large AI models” would chill R&D and investment.[9]

Moreover, determining which models pose true risks is highly complex and context-dependent. Even models developed for legitimate purposes could theoretically be misused. But that alone should not make them presumptively suspect.[10]

Rather than ill-defined technical criteria for “risky” models, the focus should be on actual malicious conduct. IaaS providers should report known or suspected malicious activities using their services, AI-related or not.[11] But legitimate AI development, even of very large models, should not be treated as inherently concerning.

---

[4] *See*, e.g., Andrew Tutt, An FDA for Algorithms, 69 Admin. L. Rev. 83 (2017).
[5] See NPRM, supra note 1, at § 7.302.
[6] *See* Andy Greenberg, *The US Government Has a Microsoft Problem*, WIRED (Aug. 13, 2023), https://www.wired.com/story/the-us-government-has-a-microsoft-problem/.
[7] NPRM, supra note 1, at § 7.308.
[8] *See, e.g.*, Ben Edwards, *OpenAI checked to see whether GPT-4 could take over the world*, Ars Technology (Mar. 15, 2023), https://arstechnica.com/information-technology/2023/03/openai-checked-to-see-whether-gpt-4-could-take-over-the-world/.
[9] *See, e.g.*, Ryan Hagemann, Jennifer Huddleston Skees, and Adam Thierer, “*Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future*,” Colorado Technology Law Journal 17 (2018): 37–130, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3118539.
[10] *See, e.g.*, Robert Gorwa & Timothy Garton Ash, *Democratic Transparency in the Platform Society*, (Aug. 16, 2022), https://osf.io/ehcy2/download.
[11] *See, e.g.*, Charles Isbell et al., *AI Algorithms Need FDA-Style Drug Trials*, WIRED (Aug. 18, 2022), https://www.wired.com/story/ai-algorithms-need-drug-trials/; NIST Risk Management Framework for AI, NIST (Aug. 18, 2022), https://www.nist.gov/itl/ai-risk-management-framework.

The U.S. must remain the most attractive environment for AI innovation. Establishing an ambiguous reporting regime for "large AI models" would undermine that critical goal and should be reconsidered.[12]

II. Enforcing Existing Laws that Already Address AI Risks

In addition to avoiding constraints on legitimate AI development, we urge the Department to recognize the robust legal frameworks that already apply to and address potential AI harms.

For example, the FTC Act prohibits unfair or deceptive practices, which the FTC has made clear covers harmful AI systems.[13] Anti discrimination laws prohibit bias in key economic areas like credit, housing, and employment, including by AI.[14] Sectoral privacy laws limit personal data use in AI systems.[15] And IP laws combat AI-related data theft.

Rather than AI-specific regulations, the focus should be ensuring existing cross-cutting laws are fully leveraged. Supporting enforcement actions by the FTC and others should be the priority.

New AI regulations would likely overlap with existing laws in confusing ways and divert focus from addressing concrete problems to definitional questions. We should allow our legal system to adapt to AI's unique challenges, not pursue a new "AI Regulatory Agency."

III. Balancing Costs and Benefits of Identity Verification

The NPRM proposes extensive identity verification requirements for IaaS providers and foreign resellers, including collecting customer information, verifying foreign customers' identities, implementing Know Your Customer programs, and filing compliance reports.[16]

While aimed at preventing IaaS use for malicious cyber activities, these requirements appear not sufficiently targeted or proportional to the risks at hand. Implementing them would be hugely burdensome for U.S. IaaS providers. Many customers might shift to foreign IaaS providers to avoid this U.S. oversight. And the reporting could itself create security risks.[17]

We urge a more risk-based approach that avoids categorical mandates and instead focuses oversight on the highest-risk contexts. Key elements could include:

---

[12] *See* Patrick Lin et al., *Robot Ethics 2.0: From Autonomous Cars to Artificial Intelligence* (2022) (discussing difficulties defining "AI" across regulatory regimes).
[13] *See* Elisa Jillson, *Aiming for Truth, Fairness, and Equity in Your Company's Use of AI*, FTC (Apr. 19, 2021), https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai.
[14] *See, e.g.*, *CFPB Issues Guidance on Credit Denials by Lenders Using Artificial Intelligence*, CFPB (Sept. 19, 2023), https://www.consumerfinance.gov/about-us/newsroom/cfpb-issues-guidance-on-credit-denials-by-lenders-using-artificial-intelligence/.
[15] *See* David Kemp et al., *Artificial Intelligence and Privacy*, IAPP (Feb. 4, 2021), https://iapp.org/media/pdf/resource_center/ai_and_privacy.pdf.
[16] NPRM, at § 7.302-04, 08.
[17] *See* John Wilson, *Cybersecurity Threats In 2023: An Expert's Top 5 Predictions*, Forbes (Dec. 22, 2022), https://www.forbes.com/advisor/personal-finance/cybersecurity-threats-for-2023/.

1. Voluntary industry best practices for identity verification[18]
2. Targeted criteria for high-risk foreign customers and activity
3. International collaboration on IaaS security norms
4. Ongoing security research to stay ahead of threats

The goal should be enhancing security while maintaining U.S. cloud industry competitiveness. Overly prescriptive unilateral requirements will not achieve that balance.

IV. Mitigating Risks of Over Reliance on Microsoft

Finally, the NPRM's provisions must be considered in light of the federal government's dangerous overreliance on a single technology provider: Microsoft. As a recent WIRED article details, Microsoft's products are ubiquitous across federal agencies, making the government uniquely vulnerable to the company's repeated major security failures in recent years.[19]

The US Government Cybersecurity & Infrastructure Security Agency's Cyber Safety Review Board said that, "During its review [of the Fall 2023 hack of government resources on Microsoft servers and software], the Board finds *that Microsoft fell short, as, for many months*, it *chose to not update* the September 6 blog that incorrectly implied that the 2016 MSA key had been stolen from a crash dump and that it had identified and corrected the issues that led to the adversary stealing the key."[20] It then said, "The Board also concludes that Microsoft's security culture was inadequate and requires an overhaul."[21]

Despite Microsoft's track record of breaches, the government appears to have little leverage to compel security improvements. Officials have not publicly criticized the company even as foreign hackers repeatedly compromise its systems. Microsoft's political savvy and market dominance have made it virtually untouchable.[22]

This is untenable. The government's dependence on Microsoft cannot mean the company gets a free pass on security. Policymakers must use every tool at their disposal, including procurement power and oversight pressure, to force changes to Microsoft's security culture.The alternative is unacceptably putting federal systems and secrets at risk.

At the same time, the government must prioritize reducing dependence on any single technology provider. Senator Wyden's proposal to shift agencies away from Microsoft's non-interoperable

[18] See, e.g., Cloud Security Alliance, Cloud Controls Matrix v4.0 (Apr. 2021), https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/.
[19] *See* Andy Greenberg, *The US Government Has a Microsoft Problem*, WIRED (Aug. 13, 2023), https://www.wired.com/story/the-us-government-has-a-microsoft-problem/.
[20] Cyber Safety Board, *Review of the Summer 2023 Microsoft Exchange Online Intrusion*, 22 (Mar. 20, 2024).
[21] *Id.* at iii.
[22] *See* Andy Greenberg, *The US Government Has a Microsoft Problem*, WIRED (Aug. 13, 2023), https://www.wired.com/story/the-us-government-has-a-microsoft-problem/.

collaboration tools is a good start.[23] CISA should also explore cloud backup solutions to avoid a single point of failure.

Ultimately, a more competitive, diverse federal IT ecosystem is essential for both security and innovation. Over reliance on Microsoft threatens to undermine both.

Conclusion

NetChoice shares the Department's goal of defending U.S. interests from malicious cyber activities. But we must pursue that objective in ways that maintain our technology leadership.

That requires safeguarding our innovative edge in AI by rejecting ill-defined restrictions on legitimate model development. It means leveraging existing legal tools to address AI risks before pursuing premature new regulations. It demands a targeted, internationally engaged approach to IaaS oversight. And it necessitates using all available policy levers to drive security improvements at major providers like Microsoft while reducing strategic vulnerability to any single company.

We appreciate the Department's consideration of these comments and look forward to further dialogue.

Respectfully submitted,

Carl Szabo
Vice President & General Counsel
NetChoice

NetChoice is a trade association that works to make the internet safe for free enterprise and free expression.[24]

[23] *See* Sen. Ron Wyden, *Wyden Releases Draft Legislation to End Federal Dependence on Insecure, Proprietary Software In Response to Repeated Damaging Breaches of Government Systems* (Apr. 8, 2024), https://www.wyden.senate.gov/news/press-releases/wyden-releases-draft-legislation-to-end-federal-dependence-on-insecure-proprietary-software-in-response-to-repeated-damaging-breaches-of-government-systems.

[24] *The views of NetChoice do not necessarily represent the views of its members.*