



October 18, 2023

Chairman Mike Collins and Ranking Member Valerie Foushee
Chairman Jay Obernolte and Ranking Member Haley Stevens
House Committee on Science, Space and Technology
Subcommittee on Investigations and Oversight and
Subcommittee on Research and Technology
2318 Rayburn House Office Building
Washington DC 20515

Re: CAIDP Statement for the Record: *Joint Committee Hearing on Balancing Knowledge and Governance: Foundations for Effective Risk Management of Artificial Intelligence, October 18, 2023*

Dear Chairman Collins and Ranking Member Foushee, Chairman Obernolte and Ranking Member Stevens, and Committee Members,

We write to you, on behalf of the Center for AI and Digital Policy (CAIDP)¹, regarding the October 18, Joint Committee Hearing on *Balancing Knowledge and Governance: Foundations for Effective Risk Management of Artificial Intelligence*.²

We previously testified on AI policy before the House Oversight Committee on *Advances in AI: Are We Ready For a Tech Revolution?*³ As CAIDP President Merve Hickok told the Committee: “We do not have the guardrails in place, the laws that we need, the public education, or the expertise in government to manage the consequences of the rapid changes that are now taking place.”⁴

¹ Center for AI and Digital Policy, <https://www.caidp.org>

² Joint Oversight & Investigations and Research and Technology Subcommittee Hearing, *Balancing Knowledge and Governance: Foundations for Effective Risk Management of Artificial Intelligence*, Oct. 18, 2023, <https://science.house.gov/2023/10/joint-oversight-investigations-and-research-technology-subcommittee-hearing-balancing-knowledge-and-governance-foundations-for-effective-risk-management-of-artificial-intelligence>

³ Testimony and statement for the record of CAIDP President Merve Hickok, *Advances in AI: Are We Ready For a Tech Revolution?* House Committee on Oversight and Accountability: Subcommittee on Cybersecurity, Information Technology, and Government Innovation (Mar. 8, 2023), https://oversight.house.gov/wp-content/uploads/2023/03/Merve-Hickok_testimony_March-8th-2023.pdf.

⁴ *Id.*

Your hearing on Foundations for Effective Risk Management could help address some of these challenges. In this statement, we respond to several of the questions set out in the hearing charter.⁵ Our recommendations in brief are:

1. Governance of AI systems should be centered on the rule of law, human rights, and democratic values
2. Congress should move forward with comprehensive AI legislation. A voluntary risk management framework is not a substitute for AI governance
3. The FTC should complete its investigation of OpenAI with urgency
4. Congress should promote the use of Privacy Enhancing Technologies (PETs) that reduce the collection and use of personal data
5. The US should lead on global AI policy and push forward the Council of Europe AI treaty

About CAIDP

The Center for AI and Digital Policy (CAIDP) is an independent research organization based in Washington, DC. We advise national governments and international organizations regarding artificial intelligence and digital policy. CAIDP currently serves as an advisor on AI policy to the OECD, the Global Partnership on AI, the European Union, the Council of Europe, UNESCO, and other national and international organizations. In April 2023, we released the third edition of our *Artificial Intelligence and Democratic Values* Index, providing a comprehensive review of AI policies and practices in 75 countries.⁶

1. What types of methods, standards, and tools currently exist for managing risks associated with AI systems?

*Established frameworks such as the Universal Guidelines for AI provide clear, implementable guidance for AI systems based on human centered values.*⁷

⁵ Committee on Science, Space, and Technology, *Balancing Knowledge and Governance: Foundations for Effective Risk Management of Artificial Intelligence*, https://republicans-science.house.gov/_cache/files/6/2/62beb7bf-0a1e-45d1-be3f-9735bb992b5d/78C980B22030E727E358E0DECFBE2545.2023-10-18-balancing-knowledge-and-governance-foundations-for-effective-risk-management-of-artificial-intelligence-hearing-charter.pdf

⁶ CAIDP, *Artificial Intelligence and Democratic Values* (2023), <https://www.caidp.org/reports/aidv-2022/>

⁷ Public Voice, *Universal Guidelines for Artificial Intelligence*, Guideline 5, <https://thepublicvoice.org/ai-universal-guidelines/>

The Universal Guidelines on AI (UGAI) were adopted in 2018 and over 330 leading experts and 60 associations (including the AAAS, the ACM, and the IEEE) have endorsed the UGAI. The UGAI sets out 12 principles that are foundational for the governance of AI systems. The aim of the Universal Guidelines is to maximize the benefits and minimize the risk of AI systems.

We advise Congress to implement these principles and move forward with governance frameworks and technical standards based on the UGAI.

2. Where do fundamental knowledge and methodological gaps exist for mitigating risks associated with AI systems?

The single most significant gap for mitigating risks associated with AI systems is the lack of federal legislation for AI. A voluntary risk management framework is not a substitute for regulations that ensure public safety. Congress should establish clear prohibitions on AI techniques that violate human rights such as mass surveillance and social scoring, mandate ex-ante human rights impact assessments for high-risk AI systems, and implement meaningful transparency measures.

We need federal AI legislation that would set standards of liability and accountability of actors in the AI life cycle. Providers of high-risk systems should be obligated to conduct ex-ante “human rights impact assessment.” Accountability mechanisms should also incorporate independent, third-party audits during the lifecycle of AI systems not just pre-deployment. Disclosure obligations should apply to public and private entities deploying AI systems and should also mandate explicit disclosure when content (including text, imagery, and other audio-visual content) is AI-generated.

Developers of foundation models as well as downstream users should be held responsible for ensuring safety by design and implementing specific safeguards on transparency of data practices and disclosure on AI-generated content. “As a part of careful data collection practices, researchers must adopt frameworks to describe the uses for which their models are suited and benchmark evaluations for a variety of conditions. This involves providing thorough documentation on the data used in model building, including the motivations underlying data selection and collection processes. This documentation should reflect and indicate researchers’ goals, values, and motivations in assembling data and creating a given model.”⁸

⁸ Emily M. Bender, Timnit Gebru, Angelina McMillan-Major, Margaret Mitchell, *On the Dangers of Stochastic Parrots: Can Language Models Be Too Big, FAccT '21*:

AI systems can replicate and amplify human biases. NIST has also reported on the problems of bias in data sets.⁹ Further, vulnerable populations are the most affected by biased AI outputs. There are examples of datasets created from human biases influencing AI to replicate systemic racism in facial recognition.¹⁰ The overriding objective of AI accountability mechanisms such as certifications, audits, and assessments should be to determine whether an AI system should be deployed. The NIST AI Risk Management Framework is voluntary, meaning that it does not set adequate and appropriate incentives for accountability.¹¹ This is critical given the individual and collective risks posed by unregulated AI systems.

Generative AI systems are built on unlicensed data, do not account for copyrights, and are already harming and marginalizing creators. In focusing investments in AI, Congress must be mindful of frameworks that result in concentration of technology in the hands of few corporations. This would severely restrict diffusion of innovation and be at cross-purposes with the U.S. National AI Research Agenda.¹²

We endorse the Hawley-Blumenthal bipartisan AI Act which offers a comprehensive framework for the governance of AI.

3. What role should the federal government play in the oversight of AI systems?

Companies should not release AI products that are not safe. President Biden has repeatedly stated that tech companies have a responsibility to make sure that their AI products are safe before making them public.¹³ OpenAI has itself acknowledged a dozen risks with ChatGPT. The federal government needs to act.

Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency (March 2021). Pages 610, 615 (Stochastic Parrots), <https://doi.org/10.1145/3442188.3445922>

⁹ *More to AI Bias than Biased Data, NIST Report Highlights*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Mar. 1, 2022), <https://www.nist.gov/news-events/news/2022/03/theres-more-ai-bias-biased-data-nist-report-highlights>.

¹⁰ *Id.*

¹¹ See U.S. Department of Commerce, National Institute of Standards and Technology, “AI Risk Management Framework,” https://airc.nist.gov/AI_RMF_Knowledge_Base/AI_RMF.

¹² CAIDP, *Statement to OSTP on US National AI Strategic Plan*, (March 4, 2022), <https://www.caidp.org/app/download/8378181763/CAIDP-Statement-OSTP-03042022.pdf?t=1660245988>

¹³ The White House, *Readout of White House Meeting with CEOs on Advancing Responsible Artificial Intelligence Innovation*, (May 4, 2023) (“President Biden dropped by the meeting to underscore that companies have a fundamental responsibility to make sure their products are safe and secure before they are deployed or made public.”), <https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/04/readout-of-white-house-meeting-with-ceos-on-advancing-responsible-artificial->

The Federal Trade Commission (FTC) should move forward and conclude its investigation of OpenAI initiated by CAIDP. Pending legislation, the Federal Trade Commission (FTC) has a unique opportunity at this time to establish guardrails for AI. Earlier this year, CAIDP filed a detailed complaint with the FTC regarding OpenAI. The FTC has opened the investigation of OpenAI we requested.¹⁴ This is clearly a positive development, but now the FTC must prioritize this investigation. It took two years from the time we filed similar complaints with the FTC concerning Google and Facebook before there was a settlement.¹⁵ We can't wait that long this time. AI products are evolving rapidly and being deployed downstream in consumer facing services. Before the end of this year the FTC must complete the investigation of ChatGPT and enter into a settlement with OpenAI that ensures the companies will abide by the practices for AI companies the Commission has previously issued.

We acknowledge (and are actively promoting) the recent announcements of several federal agencies, including NTIA, OSTP, and PCAST, to provide opportunities for public comment on AI policies.¹⁶ But even these Requests for Comments have not yet led to notice of rulemaking that would lead to regulation. Meanwhile, the OMB rulemaking to establish regulations for the use of AI across the federal government is more than two years behind schedule.¹⁷ We also note with concern that the National AI Advisory Committee (NAIAC), is lagging in its commitments under the Federal Advisory Committee Act and public comment opportunities at NAIAC have been wanting.¹⁸

[intelligence-innovation](https://www.wsj.com/articles/unite-against-big-tech-abuses-social-media-privacy-competition-antitrust-children-algorithm-11673439411); Joe Biden, *Republicans and Democrats, Unite Against Big Tech Abuses*, Wall Street Journal, (January 11, 2023), <https://www.wsj.com/articles/unite-against-big-tech-abuses-social-media-privacy-competition-antitrust-children-algorithm-11673439411>

¹⁴ Cecilia Kang and Cade Metz, F.T.C. Opens Investigation Into ChatGPT Maker Over Technology's Potential Harms, The New York Times, July 13, 2023,

<https://www.nytimes.com/2023/07/13/technology/chatgpt-investigation-ftc-openai.html>; John D. McKinnon and Ryan Tracy, *ChatGPT Comes Under Investigation by Federal Trade Commission*, Wall Street Journal, July 13, 2023, <https://www.wsj.com/articles/chatgpt-under-investigation-by-ftc-21e4b3ef>.

¹⁵ Federal Trade Commission, Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises, Nov. 29, 2011, <https://www.ftc.gov/news-events/news/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep-privacy-promises>

¹⁶ CAIDP, *Public Voice*, <https://www.caidp.org/public-voice/>

¹⁷ CAIDP Letter to Shalanda Young, Director Office of Management and Budget, Apr. 24, 2023, [hKps://www.caidp.org/app/download/8454950563/CAIDP-Statement-OMB-04242023.pdf](https://www.caidp.org/app/download/8454950563/CAIDP-Statement-OMB-04242023.pdf)

¹⁸ CAIDP *Statement to the National AI Advisory Committee* (Oct. 28, 2022), <https://www.caidp.org/app/download/8420970963/CAIDP-NAIAC-FACA-10282022.pdf>; see generally, CAIDP, *National AI Advisory Committee*, <https://www.caidp.org/resources/naiac/>

We also strongly support the notification for a rulemaking petition issued by the Federal Election Commission for reforming campaign finance laws to preserve the democratic process and election integrity from AI generated misinformation and disinformation.¹⁹ We believe that the FEC should act fast on this process and amend its regulation on fraudulent misrepresentation of campaign authority to make clear that the related statutory prohibition applies to deliberately deceptive Artificial Intelligence campaign advertisements and public communications.²⁰

4. Where should the federal government focus investments to promote the development and deployment of trustworthy AI?

The federal government should incentivize the use of Privacy Enhancing Technologies to minimize the risks of AI systems. Many machine learning systems rely on the collection of personal data. These systems can violate privacy and be used for mass surveillance. New AI systems pose new challenges for privacy, dignity, autonomy, and equality. Metrics for explainability, interpretability, and transparency should be established to protect fundamental rights, human well-being, and to increase public trust. These metrics alongside Privacy Enhancing Technologies would help protect privacy.²¹ **Privacy Enhancing Techniques (PETs) minimize or eliminate the collection and use of personal data.**

In December 2021, the Biden administration announced an initiative to encourage development of ‘Democracy-Affirming Technologies’ that support democratic values and governance. Relatedly, the U.S. and UK announced plans to promote Privacy Enhancing Technologies (PETs), including low-data AI, the deletion of unnecessary data, and techniques for robust anonymity.²²

5. How will international approaches to AI governance influence U.S. policies?

The United States should support a comprehensive treaty for the governance of AI. The EU is moving ahead with the EU AI Act and there have been a lot of proposals on AI governance

¹⁹ Federal Election Commission, *Artificial Intelligence in Campaign Ads*, 11 CFR Part 112, Notice 2023-13, Federal Register Vol. 88, No. 157, Aug. 16, 2023, <https://sers.fec.gov/fosers/showpdf.htm?docid=423639>.

²⁰ 11 C.F.R. §110.11, §11 C.F.R. 110.16. *See also*, 52 U.S.C. §30124

²¹ *Comments of CAIDP to OSTP on National Artificial Intelligence Research and Development Strategic Plan* at 4, <https://www.caidp.org/statements/> (March 4, 2022)

²² CAIDP, *Artificial Intelligence and Democratic Values Index (2022)*, pg. 1070, <https://www.caidp.org/reports/aidv-2022/>; *See also*, The White House, *US and UK to Partner on Prize Challenges to Advance Privacy- Enhancing Technologies* (December 8, 2021) <https://www.whitehouse.gov/ostp/news- updates/2021/12/08/us-and-uk-to-partner-on-a-prize-challenges-to-advance-privacy- enhancing-technologies/>



in Congress—many of which are bi-partisan.²³ The US and EU can move ahead with a transatlantic accord on AI governance which would harmonize and align the governance of high-risk AI systems.

The Council of Europe AI Treaty is “a standard-setting instrument developed through a global approach, based on international law, focusing on human dignity and human rights, as well as gender equality, social and economic justice and development, physical and mental well-being, diversity, interconnectedness, inclusiveness, and environmental and ecosystem protection can guide AI technologies in a responsible direction.”²⁴ The United States should support a comprehensive international treaty such as the Council of Europe AI Treaty.

The United States has recently rejoined UNESCO, citing the important work of UNESCO on artificial intelligence.²⁵ The U.S. should also take a leadership role in the G7 to establish common guardrails and international technical standards based on human-centered values.

Thank you for your consideration of our views. We would be pleased to provide you and your staff with additional information. We ask that this statement be included in the hearing record.

Sincerely,

Merve Hickok
CAIDP President

Christabel Randolph
CAIDP Law Fellow

Marc Rotenberg
CAIDP Executive Director

Brianna Rodriguez
CAIDP Law Fellow

²³ Marc Rotenberg, *Everything. Everywhere. All at Once: AI Policy When Congress Returns*, ACM Blog, Aug. 24, 2023, <https://cacm.acm.org/blogs/blog-cacm/275742-everything-everywhere-all-at-once-ai-policy-when-congress-returns/fulltext>

²⁴ CAIDP, Council of Europe AI Treaty, <https://www.caidp.org/resources/coe-ai-treaty/>.

²⁵ The American Independent, *Biden leads US back to membership in UNESCO*, Jun. 30, 2023, <https://americanindependent.com/joe-biden-donald-trump-china-unesco-blinken-ai/>.



Center for AI and
Digital Policy



Center for AI and
Digital Policy

ARTIFICIAL INTELLIGENCE AND DEMOCRATIC VALUES INDEX

APRIL, 2023



CENTER FOR AI AND DIGITAL POLICY
WASHINGTON, DC
CAIDP.ORG



UNIVERSAL GUIDELINES FOR AI

RIGHT TO TRANSPARENCY

All individuals have the right to know the basis of an AI decision that concerns them. This includes access to the factors, the logic, and techniques that produced the outcome.

RIGHT TO HUMAN DETERMINATION

All individuals have the right to a final determination made by a person.

IDENTIFICATION OBLIGATION

The institution responsible for an AI system must be made known to the public.

FAIRNESS OBLIGATION

Institutions must ensure that AI systems do not reflect unfair bias or make impermissible discriminatory decisions.

ASSESSMENT AND ACCOUNTABILITY

An AI system should be deployed only after an adequate evaluation of its purpose and objectives, its benefits, as well as its risks. Institutions must be responsible for decisions made by an AI system.

ACCURACY, RELIABILITY, AND VALIDITY

Institutions must ensure the accuracy, reliability, and validity of decisions.

DATA QUALITY

Institutions must establish data provenance, and assure quality and relevance for the data input into algorithms.

PUBLIC SAFETY

Institutions must assess the public safety risks that arise from the deployment of AI systems that direct or control physical devices, and implement safety controls.

CYBERSECURITY

Institutions must secure AI systems against cybersecurity threats.

PROHIBITION ON SECRET PROFILING

No institution shall establish or maintain a secret profiling system.

PROHIBITION ON UNITARY SCORING

No national government shall establish or maintain a general-purpose score on its citizens or residents.

TERMINATION OBLIGATION

An institution that has established an AI system has an affirmative obligation to terminate the system if human control of the system is no longer possible.



@THECAIDP



Center for AI and Digital Policy