December 5, 2023

Clare Martorana
U.S. Federal Chief Information Officer
Office of the Federal Chief Information Officer
Office of Management Budget
725 17th St., NW
Washington, DC 20503

Re: Request for Comments on Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence Draft Memorandum, OMB 2023-0020-0001

Dear Ms. Martorana:

The Surveillance Resistance Lab is a think and act tank focused on state and corporate surveillance as one of the greatest threats to migrant justice, racial equity, economic justice, and democracy. We challenge how surveillance at the nexus of state and corporate power not only threatens privacy, but seriously erodes fundamental rights leading to heightened oppression and repression.

While the White House's recent Executive Order on "AI"[1] technologies and the related OMB guidance promise new oversight structures for federal agencies contracting with private companies to provide "AI" services, it also risks conceding critical ground—that corporate

[1] While we use "AI" throughout our comment to maintain consistency with OMB's proposed guidance, we must name that the adoption of marketing language like "AI" or "artificial intelligence" by the government as the shorthand term used to describe regulation and governance of a variety of different automated decision-making tools contributes to public and consumer confusion about what "AI" is and is not. As Luis Perez-Breva, lecturer and research scientist at MIT School of Engineering, observes, "I see a rush to over-market as AI anything that involves computation with data. That just sows a lot of confusion. Things advertised as "AI" today have no intelligence of their own." Greg Nichols, Don't be alarmed, but you're probably using the term AI wrong | ZDNET, Nov. 15, 2017. Available at: https://www.zdnet.com/article/dont-be-alarmed-but-youre-probably-using-the-term-ai-wrong/,

needs, and not the public's, will drive agencies' governing strategies. The guidance privileges "innovation" at the expense of the public sector.[2]

The public and government's ability to hold contractors accountable for harm caused by safety and rights-impacting "AI" systems is already diluted by laws that protect corporations from transparency, oversight, and accountability mechanisms necessary for the public to understand and influence governance. For example, government contractors sued for violating the United States Constitution or other laws through the services they provide the government may invoke the "government contractor defense", limiting the public's access to the courts for remedies of constitutional magnitude.[3] Public notice and comment opportunities through administrative agencies, like this one, are not required before the procurement of technologies, even when policy decisions are embedded in the design of such technology.[4] Government agencies are also already exempt from disclosing information to the public and investigative media via Freedom of Information Act exemptions, such as Exemption 4, which exempts "trade secrets and commercial or financial information obtained from a person and privileged or confidential" from disclosure.[5]

As "AI" produced by the private sector becomes increasingly embedded and deployed by government institutions, we must take forceful action to ensure that the public interest values of transparency, inclusivity, reasonableness, and political equity[6] are not eroded by profit-driven corporate imperatives of secrecy, scarcity, competition, and market-driven metrics. To protect the public's need over corporate interests, we must guard against corporate attempts to dominate narratives related to product performance and conditions in the public sector that impact investments as well as "risk management" approaches to protecting the public.

AI is being fueled by a handful of extremely well resourced corporations who are in a fierce competition to define our futures.[7] The chaos that resulted from OpenAI's three-person Board of Directors decision over one weekend firing and rehiring its CEO, for example, is exactly the type of corporate theater that may impact the future of AI governance technologies behind closed doors.[8]

---

[2] The Lab also echoes similar concerns made by the Athena Coalition.
[3] Boyle v. United Technologies Corp., 487 U.S. 500, 512 (1988).
[4] Mulligan, Deirdre K. and Bamberger, Kenneth A., Procurement As Policy: Administrative Process for Machine Learning (October 4, 2019). Berkeley Technology Law Journal, Vol. 34, 2019, at 788. Available at SSRN: https://ssrn.com/abstract=3464203 or http://dx.doi.org/10.2139/ssrn.3464203
[5] Food Marketing Institute v. Argus Leader Media, 139 S. Ct. 2356, 204 L. Ed. 2d 742 (2019), citing 5 U.S.C. § 552(b)(4).
[6] Iris Marion Young, *Inclusion and Democracy,* Oxford Press (2000) 23-25
[7] Cade Metz, Karen Weise, Nico Grant and Mike Isaac, "Ego, Fear and Money: How the A.I. Fuse Was Lit", N.Y. Times, Dec. 3, 2023. Available at: https://www.nytimes.com/2023/12/03/technology/ai-openai-musk-page-altman.html. "Mr. Musk, Mr. Page, Mark Zuckerberg of Meta, the tech investor Peter Thiel, Satya Nadella of Microsoft and Sam Altman of OpenAI. All have fought for a piece of the [AI] business — which one day could be worth trillions of dollars — and the power to shape it."
[8] Justin Hendrix, The Saga at OpenAI: Lessons for Policymakers, Tech Policy Press, Nov. 26, 2023. Available at: https://techpolicy.press/the-saga-at-openai-lessons-for-policymakers/. In this interview, Justin Hendrix's observes, "That does seem to be the conclusion of [Karen Hao's] piece the other day, even

Other examples of how corporate imperatives begin to trump constitutional and public interests include a lawsuit brought by teachers in Houston who sued their school district for constitutional due process violations related to using a privately-developed performance algorithm to evaluate teachers for pay and continued employment. When they demanded information about how the system made their employment action decisions, the company claimed trade secret privilege to prevent disclosure of information the teachers were entitled to.[9] In criminal courts across the country, where explicit constitutional rights of confrontation protect the accused's right to access information, private technology companies have argued against allowing defense experts access to the mechanics behind their system's outcomes.[10]

By committing to the outsourcing of "AI" services and a "risk management" approach to enforcement of public constitutional and statutory protections[11] through procurement and contract monitoring, the federal government has already chosen to fundamentally

---

though this may have seemed like a crazy moment with OpenAI possibly falling apart, possibly somehow being folded into Microsoft, now, it appears, carrying on as an independent entity, but very much under the puppet strings of Microsoft. One detail that I hadn't really quite understood was the extent to which the $10 billion investment Microsoft's made in OpenAI is really for computing resources, almost like a barter, which is interesting. Just like any old startup taking credits from Amazon or Microsoft, OpenAI is in this similar boat, hooked on its cloud compute infrastructure. This idea that, at the end of the day, there's only a handful of folks in Silicon Valley that are defining the future of these technologies, that are making the decisions." Karen Hao responds: **"And that is, I think, the most important lesson that we need to learn from this weekend, and that policymakers should very much be realizing, and I hope acting on,** which is if we actually want to get to a place where, if we believe the general premise that OpenAI says, which is, we're building [artificial general intelligence (or "AGI")] that's beneficial for humanity, if we actually want something like that, setting aside skepticism around AGI or whatever, but a technology that benefits everyone can only arise when there is a broad base of people participating in it and helping to usher it forward in an inclusive and democratic way. And that's just absolutely not… It's like the polar opposite extreme that's happening. The fact that it really came down to three members of a board that led to the cascading of these events, three people that could completely fundamentally change the direction of AI development, …and all of those discussions are happening behind closed doors, and t is not healthy or sustainable in terms of getting to a future that is better and more inclusive."

[9] Tom Temin, "How federal procurement can keep artificial intelligence in its swim lane," Federal News Network, Nov. 3, 2023. Available at: https://federalnewsnetwork.com/artificial-intelligence/2023/11/how-federal-procurement-can-keep-artificial-intelligence-in-its-swim-lane/. In this interview with University of Pennsylvania law professor and federal regulation expert Cary Coglianese, Prof. Coglianese reports, "But back several years ago, the school teachers in the city of Houston took the school district to court, because the school district had been applying a performance algorithm that was being used to evaluate teachers for pay and continued employment. The algorithm had been developed and was run by a private contractor who claimed trade secret protection over the algorithm. And the teachers said, Wait a minute, we're public employees, school district, you're a public entity. We have constitutional due process rights to some degree of transparency and fairness in how we are being evaluated. And we can't even know what that is. And the court agreed with them. **And it seemed to me, in retrospect, an obvious fix for that would have been to have the school district during the contracting process require the vendor to provide adequate information**." See also "Litigating Algorithms - AI Now Institute," Section Three: Public Teacher Employment Evaluations (2018) Available at: https://ainowinstitute.org/publication/litigating-algorithms-3

[10] Rebecca Wexler, "Code of Silence", Washington Monthly, Jun. 11, 2017. Available at: https://washingtonmonthly.com/2017/06/11/code-of-silence/

[11] OMB guidance Section 6 (p24)

weaken public access to transparency and accountability mechanisms.[12] In addition, OMB's guidance to agencies around "workforce"[13] that prioritizes administrative agency staff hiring for people with "AI" interpretation skills rather than the subject-matter expertise of that agency's focus will gut its internal staff subject-matter expertise capacity and legitimacy.[14] Undermining the authority of federal administrative agencies further serves technology companies future interests–for example, Meta (formerly known as "Facebook") is already actively seeking to limit the enforcement power of federal agencies through litigation.[15]

Given this relinquishment of traditional mechanisms for public accountability, it is critical that the OMB Guidance on "AI" create clear mandates and open avenues for public transparency, intervention, and accountability in order to preserve the public's right to learn about and intervene against "AI" companies involved in governing their lives, especially in ways that increase risks to safety and not only individuals' constitutional rights, but communities' rights to protect their future. **Instead, the guidance opens avenues for unprecedented opacity around corporate influence in government through extension and waiver loopholes allowing "AI" corporations to withhold critical information about governing without oversight or consequences.**

Language around waivers should be eliminated entirely – this creates a dangerous loophole through which the government may not only withhold information from the public without a declassification process, but evade the process of the minimum impact assessments in full. This invites companies to market their services as high risk for the purposes of avoiding AI impact assessments. For exceptional situations, agencies should use existing classification standards.

Where possible, the guidance should also offer model contract language to mitigate the potential of interpretations that weaken the effectiveness of these provisions. Examples of model contractual provisions may be found in Confronting Black Boxes, A Shadow Report of the New York City Automated Decision-making Task Force.[16]

---

[12] The Lab co-authored, along with other immigration advocacy organizations, a public comment addressing the specific reasons why a risk management framework dilutes accountability and inappropriately assigns agencies like the Department of Homeland Security the duties of self-policing their use of AI and its harms despite already demonstrating its inability to do so.

[13] Section (4)(b)(iv)

[14]Ryan Calo & Danielle K. Citron, The Automated Administrative State: A Crisis of Legitimacy, 70 Emory L. J. 797, 804 (2021). Available at: https://scholarlycommons.law.emory.edu/elj/vol70/iss4/1, "Mounting evidence suggests that agencies are turning to systems in which they hold no expertise, and that foreclose discretion, individuation, and reason-giving almost entirely. The automated administrative state is less and less the imperfect compromise between the text of the Constitution and the realities of contemporary governance. **At some point, the trend toward throwing away expertise, discretion, and flexibility with both hands strains the very rationale for creating and maintaining an administrative state. This is especially true where, as often, the very same processes of automation also frustrate the guardrails put in place by Congress and the courts to ensure agency accountability.**"

[15] The Associated Press, "Facebook parent Meta sues the FTC claiming 'unconstitutional authority' in child privacy case", ABC News, Nov. 30, 2023. Available at: https://abcnews.go.com/Politics/wireStory/facebook-parent-meta-sues-ftc-claiming-unconstitutional-authority-105288850

[16] Rashida Richardson, ed., "Confronting Black Boxes: A Shadow Report of the New York

Below are more specific recommended amendments (in order of importance) to strengthen the public's ability to hold federal agencies accountable for threats to safety and rights posed by government contractors' when procuring "AI" services.

(1) Amend (5)(d)(i)(p21) to make agencies contractually bind "AI" companies to uphold the United States Constitution and laws. Clarify that entities operating "AI" on behalf of the government will be designated as state actors.

> Current OMB Guidance:
>
> Aligning to National Values and Law. Agencies should ensure that procured AI exhibits due respect for our Nation's values, is consistent with the Constitution, and complies with all other applicable laws, regulations, and policies, including those addressing privacy, confidentiality, copyright, human and civil rights, and civil liberties.
>
> Recommended amendment:
>
> Aligning to National Values and Law. Agencies **must ensure that federal contracts for** procured AI **bind companies to uphold** the Constitution, and comply with all other applicable laws, regulations, and policies, including those addressing privacy, confidentiality, copyright, human and civil rights, and civil liberties. **Government contracts with entities operating "AI" on behalf of the government shall designate the contractor as a state actor. All existing contracts with companies providing "AI" services must be updated to reflect this expectation.**

Without binding contractual language, agencies have little power to force government contractors to "exhibit[] due respect" for the constitution, laws, regulations, and policies, and the public has even less. Requiring government contractors to adopt state actor status will protect the public's ability to access the courts to remedy harms caused by new technologies. "[The] applicability of the state action doctrine to AI vendors and their systems will be a central question for AI accountability going forward."[17] OMB guidance should preserve the public's ability to have standing and file for both remedial and injunctive relief from deployment of harmful technology. Not doing so dangerously insulates both government contractors and government actors from important venues for public accountability.

City Automated Decision System Task Force," AI Now Institute, December 4, 2019, Available at https://ainowinstitute.org/publication/confronting-black-boxes-a-shadow-report-of-the-new-york-city-automated

[17] Kate Crawford and Jason Schultz, 2019 'AI Systems As State Actors', Columbia Law Review, 119(7), 1941-1972, 1958. Available at: https://columbialawreview.org/content/ai-systems-as-state-actors/

(2) Amend (5)(c)(iii)(p14) to align the circumstances when CAIO's may waive minimum protective practices for safety and right-threatening technologies with existing classification processes

> Current OMB Guidance:
>
> Waivers from Minimum Practices. In coordination with other relevant officials, an agency CAIO may waive one or more of the requirements in this section for a specific covered AI application or component after making a written determination, based upon a system-specific risk assessment, that fulfilling the requirement would increase risks to safety or rights overall or would create an unacceptable impediment to critical agency operations. Such waivers are applicable for the duration of the AI's use, but must be reassessed by the CAIO if there are significant changes to the conditions or context in which the AI is used. An agency CAIO may also revoke a previously issued waiver at any time. Agencies must report to OMB within 30 days of granting such a waiver, detailing the scope, justifications, and supporting evidence.
>
> Recommended amendment:
>
> ~~Waivers from Minimum Practices. In coordination with other relevant officials,~~ **If an agency CAIO determines that fulfilling the minimum practices would increase risks to safety or rights overall or would create an unacceptable impediment to critical agency operations, the CAIO must nevertheless complete the AI assessment and apply for an AI system's impact assessment to be classified under existing classification standards and procedures in Executive Order 13256.**

Rather than allowing agencies to evade production of AI assessments without a declassification process, OMB should deploy existing structures, such as the classification (and declassification) system, to determine what information cannot be shared publicly, why, and for how long. Through this guidance, OMB risks encouraging that agencies govern by waiver (or, as many FOIA officers do, by endless extensions) and that technology companies market their products as systems whose impact assessments may be waived. New understaffed offices will be tempted to overuse system-specific risk assessments to grant extensions and waivers as short cuts around the rigorous and more laborious task of completing the AI impact assessments.

In addition, the most potentially harmful technologies that are being deployed already by federal law enforcement and state and local law enforcement with the support of federal dollars foreseeably will seek to exempt their technologies from the Minimum Practices, along with the companies marketing these dangerous technologies. New Yorkers saw this exact opposition when the New York City Council passed a bill requiring city agencies to similarly inventory their algorithmic decision-making systems.[18] New York City's Police Department testified and complained to the media that "compliance with the legislation would 'help criminals and

[18] Richardson at 11-13.

terrorists.'"[19] As we wrote alongside the immigration coalition organizations in another letter, law enforcement has already proven it is incapable of critically assessing the life-threatening and community-devastating corporate technologies it has already deployed. The government should not evade the process of assessing the risks of any type of AI system so that potential harms are primarily identified early and avoided and, in the event harm results, the government's knowledge of the risk of harm and the company's knowledge about the risk of harm are well-documented and undisputed.

We echo the third concern of the immigration coalition organizations: "we are concerned that intelligence and law enforcement-related technologies will fall under 'critical agency operations,' allowing agencies to avoid scrutiny, and enabling the procurement and implementation of harmful technologies that do not meet minimum standards. We are additionally concerned about these issues being relegated to the National Security Memo where they could receive even less public scrutiny."[20]

(3) Amend (5)(c)(iv)(A)(1)(p15) to require articulation of the problem "AI" is sought to solve, public engagement about that problem, and to rule out less harmful alternatives to "AI"

Current OMB Guidance:

The intended purpose for the AI and its expected benefit, supported by specific metrics or qualitative analysis. Metrics should be quantifiable measures of positive outcomes for an agency's mission, for example to reduce costs, wait time for customers, or risk to human life, that can be measured after the AI is deployed to confirm or disprove the value of using AI. Where quantification is not feasible, qualitative analysis should demonstrate an expected positive outcome, such as for improvements to customer experience or human interactions—and demonstrate that AI is a good fit to accomplish the relevant task.

Recommended amendment:

The intended **problem that AI is being proposed to solve and efforts to engage the public about the priority of that problem, the exhaustion of government-led strategies, the history of government attempts to solve this problem, identification of specific reasons why this particular problem might be addressable through outsourcing AI services. The assessment of the problem must also include and document public, civil society, and other stakeholder input gathered through notice and comments. It should also document the** purpose for the AI and its expected benefit, supported by specific metrics or qualitative analysis. Metrics should be quantifiable measures of positive outcomes for an agency's mission, for example to

[19] Id. at 12
[20] Public comment submitted by Just Futures Law, et al at 2.

reduce costs, wait time for customers. **If risk to human life is projected**, **the AI should not be deployed.** Where quantification is not feasible, qualitative analysis should demonstrate an expected positive outcome such as for improvements to customer experience or human interactions **weighed against any negative outcomes**—and demonstrate that AI is a good fit to accomplish the relevant task. **If measures required to mitigate risk, for example human review, dilutes any "efficiencies" initially deemed positive, this should be included.**

Whether or not this problem is a priority, and whether technology promises the appropriate solution, not only to the agency programmatic staff, but to its constituents and the people who will be subjected to the technology, is left out of the AI assessment. How is risk to human life a positive outcome for any agency's mission, for example? It is during the process of defining a problem, understanding what conditions need to change in order to solve it that an agency can better prepare itself for a future assessment of whether AI is the right solution, whether the problem is not a priority, or whether alternatives should be used.

(4) Amend (5)(b)(i)(J)(p10-11) to broaden the types of safety-impacting risks the minimum practices must be presumed to apply to

Current OMB guidance:

Access to or security of government facilities;

Recommended amendment:

Access to or security of government facilities **or places where people live**

Nothing in the current list of safety-impacting threats speaks to the safety of people, whether in the United States or elsewhere. Weaponized AI systems absolutely have the ability to threaten the safety of individuals and entire communities and should be included in this list.

(5) Amend (5)(b)(ii)(p12) to broaden the types of rights-impacting risks the minimum practices must be presumed to apply to

Current OMB guidance:

Purposes That Are Presumed to Be Rights-Impacting. Unless the CAIO determines otherwise, covered AI is presumed to be rights-impacting (and potentially also safety-impacting) and agencies must follow the minimum practices for rights-impacting AI and safety-impacting AI if it is used to control or meaningfully influence the outcomes of any of the following activities or decisions:

Recommended amendment:

> Purposes That Are Presumed to Be Rights-Impacting. Unless the CAIO determines otherwise, covered AI is presumed to be rights-impacting (and potentially also safety-impacting) and agencies must follow the minimum practices for rights-impacting AI and safety-impacting AI if it is used to control or meaningfully influence the outcomes of any of the following activities or decisions **about individuals or communities**:

This recommendation echoes a concern also raised in the comment we co-authored along with other immigration justice organizations: "OMB should consider including the concept of collective privacy because worker and labor organizing or immigrants rights advocacy often mean that individual privacy and collective privacy are intertwined. Reducing the risk of retaliation against labor organizing or people engaged in protected First Amendment activity requires assessing the needs of organizing collectives engaged in that enterprise."[21]

Conclusion

The federal government has already chosen to fundamentally weaken public access to transparency and accountability mechanisms by privileging corporate-driven outsourcing of public sector responsibilities. Given this relinquishment of traditional mechanisms for public accountability, the OMB Guidance on "AI" must create clear mandates and require open avenues for public transparency, intervention, and accountability in order to preserve the public's right to learn about and intervene against "AI" companies involved in governing their lives, especially in ways that increase risks to safety and not only individuals' rights to self-determination, but communities' rights to protect their future. There must be consequences for non-compliance, overuse of waivers and extensions, contract monitoring and enforcement, and oversight of agencies' engagement in monitoring "AI" systems.

Thank you,

Surveillance Resistance Lab

[21] Id. at p10-11