Initial Analysis of the new U.S. governance for Federal Agency use of Artificial Intelligence, including biometrics

Pam Dixon, Executive Director

28 March 2024

Today the Biden-Harris Administration published a Memorandum that sets forth how U.S. Federal Agencies and Executive Departments will govern their use of Artificial Intelligence in its Office of Management and Budget (OMB) Memorandum M-24-10, *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence* (March 28, 2024). The memorandum implements Executive Order 14110 on AI, which directed its publication. The memorandum creates extensive AI governance requirements ranging from how procurement of AI systems is conducted to risk assessment of AI and informing the public and giving the public choice in regards to some government uses of AI. The memorandum applies to all agencies as defined in 44 U.S.C and the *AI in Government Act of 2020*, and excludes elements of the Intelligence Community. A separate memorandum is being prepared to be applicable to the use of AI for national security purposes.

WPF commented extensively on the draft memorandum when it was open for public comment in 2023. On March 27, 2024, WPF's executive director Pam Dixon and deputy director Kate Kaye attended a White House briefing for civil society on the final version of the memorandum, where there was an opportunity to ask questions.

The OMB memorandum provides an extensive and in some ways surprising articulation of emergent guardrails around modern AI. There are many points of interest to discuss, but the most striking includes the thread of biometrics systems guidance throughout the memorandum and continuing on in the White House Fact Sheet and associated

materials. Additionally, the articulation of minimum practices for safety -impacting and rights- impacting AI will likely become important touch points in regulatory discussions in the U.S. and elsewhere.

First and foremost for this discussion, the memorandum establishes minimum practices for "Safety-impacting and rights-impacting Artificial Intelligence." The practices that the OMB has outlined must be applied by December 1, 2024 or the agency must stop using AI. The required practices are extensive, and include an expansion of the discussion of AI Impact Assessments and how they are to be conducted throughout the AI lifecycle, notably including assessment of AI systems using metrics, which the memorandum notes should be "quantifiable measures of positive outcomes for the agency's mission," in addition to other measures. WPF's December 2023 report, *Risky Analysis: Assessing and improving AI governance tools,* discusses such metrics in detail, and provides a global index of these nascent tools and measures.

The memo includes additional minimum practices for rights-impacting AI such as requirements for consulting and incorporating feedback from affected communities and the public. For example:

> "B. Consult and incorporate feedback from affected communities and the public. Consistent with applicable law and governmentwide guidance, agencies must consult affected communities, including underserved communities, and they must solicit public feedback, where appropriate, in the design, development, and use of the AI and use such feedback to inform agency decision-making regarding the AI The consultation and feedback process must include seeking input on the agency's approach to implementing the minimum risk management practices established in Section 5(c) of this memorandum, such as applicable opt-out procedures." (Page 22.)

The discussion of opt-out here is notable, because the memorandum explicitly includes the Federal government's use of biometrics as an AI use case that impacts rights. In such cases, Agencies using face recognition and other biometric systems are specifically and clearly directed to take extensive extra steps, which will encompass the expanded AI Impact Assessments, public feedback, monitoring for discrimination, providing notice to affected members of the public, and additional responsibilities.

The biometric use case runs as a thread throughout the memorandum. For example, biometrics is also expressly discussed in the memorandum's section on responsible procurement. This section requires the government to assess when or if biometric information was collected without consent, was collected for other purposes originally, or was collected without validation of identity. The memorandum also requires "documentation or test results" regarding biometric systems' accuracy, validity, and "reliability to match identities." From the memorandum:

> "Responsible Procurement of AI for Biometric Identification. When procuring systems that use AI to identify individuals using biometric identifiers e.g., faces, irises, fingerprints, or gait — agencies are encouraged to:
>
> A. Assess and address the risks that the data used to train or operate the AI may not be lawfully collected or used, or else may not be sufficiently accurate to support reliable biometric identification. This includes the risks that the biometric information was collected without appropriate consent, was originally collected for another purpose, embeds unwanted bias, or was collected without validation of the included identities; and
>
> B. Request supporting documentation or test results to validate the accuracy, reliability, and validity of the AI's ability to match identities." (pages 25-26)

The discussion of biometrics guardrails does not stop at the memorandum. In the corresponding Fact Sheet released by the White House that explained the memorandum, the TSA's use of face recognition in airports is specifically called out, noting that, if the safeguards in the guidance are appropriately adopted, it could ensure that "When at the airport, travelers will have the ability to opt out from the use of TSA facial recognition without any delay or losing their place in line." This statement, coming directly from the White House, taken together with the extensive requirements in the memorandum, should be a clear call to every biometric developer, vendor, deployer, and end user that a seismic policy shift has taken place. If biometrics will be used, non-consensual training data will be a problem as will bias, untested or unvalidated systems. An initial and ongoing in-depth AI Impact Assessment is required, as is the provision of consumer redress and other transparency and trustworthiness measures.

The memorandum's statement of how biometrics should be deployed in Federal use cases is by far the most assertive, clear, and direct articulation of biometric governance by the U.S. government to date. It may potentially be the most astute articulation of biometric governance in regards to AI-specific requirements and guardrails applicable to a national government anywhere to date. WPF will be doing additional analysis on this point, but on first blush, because the U.S. government is not broadly exempted from requirements for the minimum practices, the specific remediations stand to have potentially significant positive impact. Regardless of extra-territorial comparisons, the memorandum sets a critically important and improved precedent in this aspect of AI governance, and will make inappropriate uses of biometrics by the U.S. Federal government or the procurement of unethically sourced or unverified biometric systems extremely difficult to support going forward.

Other key exemplars of AI uses that are deemed rights-impacting AI include AI uses in Federal healthcare systems. Here, the memorandum requires assuring human oversight and attention to disparities in access to healthcare. Another included use case for rights-impacting AI is when AI is used to detect fraud. Here, the memorandum's safety-impacting and rights-impacting guidance directs agencies to ensure human

oversight of impactful decisions and to ensure that impacted individuals are able to seek redress for AI harms.

The memorandum contains a lot of moving parts, and there is much more to say about it. Overall, though, the memorandum marks an important and coherent articulation of what is likely the beginning of the building of socio-technically and ethically informed guardrails for modern forms of AI, including biometrics systems. Building modern, fit-for-purpose AI guardrails is not an easy task given the complexity of modern systems combined with the stark growth rate of AI development today. Nevertheless, this memorandum provides necessary and clear guidance for the Federal government regarding the use of AI. Even if some quibble about aspects of the guidance, taken as a whole, it represents a significant advancement in regulatory guidance and protective guardrails for the public that are adapted to the today's socio-technical contexts and needs.