Policy Recommendations for the Responsible Use of Artificial Intelligence

June 2024

Data & Trust Alliance

As regulators and policymakers around the world try to understand, define and control Artificial Intelligence, Machine Learning and Generative Artificial Intelligence, the number of approaches, methods and requirements are varied and challenging for business enterprises to navigate as they continue to innovate and develop new products and services. The simultaneous evolution of regulatory requirements and innovations creates an environment that can be difficult to navigate even when most organizations and governments have the same goals in mind: to build a future that creates net benefits for individuals, communities and society as a whole. To navigate this challenging moment in time takes dedication, focus on governance and a commitment to trusted data and analytic practices.

The Data & Trust Alliance, an organization of world-class business enterprises, created this policy recommendation document as a first step in providing guidance to all stakeholders as we attempt to create a positive future that effectively accesses these new technologies. We hope these recommendations are constructive as society and innovation progress and we look forward to examining these and other topics in more detail.

Published 06.13.24

Authored by the AI Policy Working Group of the Data & Trust Alliance

❶ Regulate AI risk, not AI algorithms.

We believe that AI should be explainable, fair, robust, transparent, and privacy protective in a manner commensurate with the risk of the intended uses and purposes of the AI system. This assertion means that we:

1A

Support an approach that regulates use of AI in high-risk applications.

Regulation should encourage innovation while mitigating risk, based on the intended use-cases and purposes, taking into account factors such as the application(s), end-user(s), how reliant the end-user would be on the technology, and the level of human oversight. Accordingly, we support policy that would:

- Provide explicit categories with sets of high-risk AI use cases for which regulations would apply in order to provide clarity and predictability to AI developers, deployers and the public;
- Mandate impact assessments and bias testing for high-risk AI use cases;
- Require transparency, defined by users knowing when they are interacting with an AI system within a high-risk use case and whether they have recourse to engage with a real person, if desired. Also, encourage explainability, where appropriate and commensurate

with the risk, to give society better visibility and greater assurances into how these models operate.

- Where appropriate and commensurate to the risk, AI developers should be required to disclose technical information about the development and performance of an AI model related to the use case(s) in order for deployers to conduct the requisite impact assessments and bias testing, as well as the empirical data sources used to train it, to give society better visibility and greater assurances into these models;

- Prevent and stop harm. Take measures so that AI systems are not leveraged for specific prohibited uses that present a significant risk of harm. These prohibitions include the use of AI for mass surveillance, racial profiling, and violations of basic human rights and freedoms;

- Ensure AI developers and deployers employ "trustworthy" AI governance including safety, privacy, disclosure, data quality, etc., which may include, where appropriate, leveraging the NIST AI Risk Management Framework and its best practices around these trustworthy AI qualities and/or the White House Voluntary AI Commitments for Generative AI. Good AI governance should be calibrated for the specific risks and use cases, and may include:

  → Built and tested for safety; continue to develop and apply strong security practices to avoid unintended results that create harm.

  → Incorporate privacy design principles, give opportunity for notice and consent for consumers.

  → Enable appropriate disclosure when personal information is processed for automated decision-making or profiling impacting matters of significance, including options to elect human review or alternative processing.

  → Development of cross-sector data provenance standards to ensure trustworthy data and to reject sources of data, deemed to be untrustworthy (D&TA effort underway).

Please see included addendum, "Notable AI, Cybersecurity, and Privacy Commitments by D&TA Members" (individually and via association groups).

Learn more about the Data & Trust Alliance

1B

Avoid government "AI license to operate" obligations

Mandatory government licensing and pre-market deployment certification and requirements—particularly when applied to non-high risk AI systems—have significant economic costs, stifle competition, and reduce the availability of opensource AI systems. Policymakers should recognize:

- AI value chains are complex and constantly evolving. Requiring a license from the government at any point in this value chain would create an enormous obstacle to its efficient operation.