July 7, 2023

Office of Science and Technology Policy
Eisenhower Executive Office Building
725 17th Street NW
Washington, District of Columbia 20502

RE: Comments of ACT | The App Association to the White House's Office of Science and Technology Policy on *Request for Information; National Priorities for Artificial Intelligence* (88 FR 34194; OSTP-TECH-2023-0007)

ACT | The App Association (App Association) appreciates the opportunity to provide input to the Office of Science and Technology Policy (OSTP) on national priorities to inform the development of a National Artificial Intelligence (AI) Strategy.[1]

The App Association is a global trade association for small and medium-sized technology companies. Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem that engage with verticals across every industry. We work with and for our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology. Today, the value of the ecosystem the App Association represents—which we call the app economy—is approximately $1.8 trillion and is responsible for 6.1 million American jobs, while serving as a key driver of the $8 trillion internet of things (IoT) revolution.[2] Alongside the world's rapid embrace of mobile technology, our members create the innovative solutions that utilize AI to power IoT across various modalities and segments of the economy.

AI is an evolving constellation of technologies that enable computers to simulate elements of human thinking, such as learning and reasoning. An encompassing term, AI entails a range of approaches and technologies, such as machine learning (ML), where algorithms use data, learn from it, and apply their newly-learned lessons to make informed decisions, and deep learning, where an algorithm based on the way neurons and synapses in the brain change as they are exposed to new inputs allows for independent or assisted decision-making. AI-driven tools are having, and will continue to have, substantial direct and indirect effects on Americans. Some forms of AI are already being used to improve American consumers' lives today – for example, AI is used to detect financial and identity theft and to protect the communications networks upon which Americans rely against cybersecurity threats. Moving across use cases and sectors, AI has incredible potential to enable faster and better-informed decision making

[1] 88 FR 34194.

[2] ACT | The App Association, State of the U.S. App Economy: 2020 (7th Edition) (Apr. 2020), available at https://actonline.org/wp-content/uploads/2020-App-economy-Report.pdf

through cutting-edge distributed cloud computing. For example, healthcare treatments and patient outcomes stand poised to improve disease prevention and conditions, as well as efficiently and effectively treat diseases through automated analysis of x-rays and other medical imaging. From a governance perspective, AI solutions will derive greater insights from infrastructure and support efficient budgeting decisions.

Today, consumers are encountering AI in their lives incrementally through the improvements they have seen in computer-based services they use, typically in the form of streamlined processes, image analysis, and voice recognition, all forms of what we consider "narrow" AI. These narrow applications of AI already provide great societal benefit. As AI systems, powered by streams of data and advanced algorithms, continue to improve services and generate new business models, the fundamental transformation of economies across the globe will only accelerate. Nonetheless, AI's growing use raises a variety of challenges, and some new and unique considerations, for policymakers as well as those making AI operational today. The App Association appreciates OSTP's efforts to develop a National AI Strategy that provides reliable guidance to stakeholders to reassure end-users that AI systems are legal, effective, ethical, safe, and otherwise trustworthy.

The App Association has worked proactively to develop consensus around AI governance and policy questions from across its diverse and innovative community of small businesses. As a result of these consensus-building efforts, the App Association has created comprehensive policy principles for AI governance[3] which address many of the areas raised by OSTP in its request for information with detailed recommendations. Notably, the App Association's policy principles for AI address quality assurance and oversight, recommending that any AI policy framework utilize risk-based approaches to ensure that the use of AI aligns with the recognized standards of safety, efficacy, and equity. Our AI policy principles also prioritize ensuring the appropriate distribution and mitigation of risk and liability by providing that those in the value chain with the ability to minimize risks based on their knowledge and ability should have appropriate incentives to do so.

The App Association also strongly urges for a coordinated effort across both executive and independent agencies. Already, numerous regulatory agencies, some cross-sectoral and others sector-specific, are considering or advancing regulatory proposals that would take starkly different approaches to AI accountability. Some of these proposals are poised to put significant hurdles in place for the development and use of AI through one-size-fits -all approaches that have nominal public benefit at best and are misaligned with other leading Administration efforts, such as that of the National Institute of Standards and Technology [NIST][4]). In some cases, such proposals are

[3] The App Association's Policy Principles for Artificial Intelligence are included in this comment as **Appendix A**.

[4] https://www.nist.gov/itl/ai-risk-management-framework.

being developed based on speculative and undemonstrated harms.[5] OSTP, along with other cross-sectoral subject matter expert agencies in the federal government such as NIST, should take needed steps through the future National AI Strategy to ensure a harmonized and informed approach to AI governance.

Many entities, both public and private, are actively engaging in efforts to create and enforce AI accountability frameworks, which may lead to the creation of trusted audits, assessments, and certifications. While this area continues to evolve, we strongly urge for OSTP's alignment with NIST's efforts to develop a voluntary artificial intelligence risk management framework (AI RMF), which aims to help designers, developers, users, and evaluators of AI systems evolve in knowledge, awareness, and best practices to better manage risks across the AI lifecycle.[6] NIST's AI RMF is best positioned to guide federal government efforts in addressing AI due to NIST's expertise and its collaborative and open approach to developing the AI RMF, similar to NIST's Cybersecurity Framework.[7] It is in the public's best interest that the NIST AI RMF's scaled, risk-based approach serve as a basis for both executive and independent agencies' approach to AI risk management and governance; and that OSTP take active steps to bring federal agencies into alignment with this approach.

[5] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 FR 51273 (Aug. 22, 2022); App Association views provided to the Federal Trade Commission in response to its Advanced Notice of Proposed Rulemaking are available at https://www.regulations.gov/comment/FTC-2022-0053-1089.

[6] https://www.nist.gov/itl/ai-risk-management-framework.

[7] https://www.nist.gov/cyberframework.

The App Association appreciates OSTP's consideration of the above (and appended) views, and we urge OSTP to contact the undersigned with any questions or on ways that we can assist moving forward.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Leanna Wade
Regulatory Policy Associate

ACT | The App Association
1401 K St NW (Ste 501)
Washington, DC 20005
202-331-2130

APPENDIX A

Policy Recommendations for AI

ACT
The App Association

Artificial Intelligence (AI) is clearly a priority for policymakers, with 37 AI-related laws enacted globally, more than 80 pending legislative proposals at the state level and several more at the federal level. To understand and shape rules for this complex and evolving technology, a vital voice—that of small businesses, members of ACT| The App Association—must be prioritized in order to create a competitive, safe, and secure AI future.

We initially released these principles in 2021. However, we are updating them continually to reflect new developments in privacy and data security laws around the world and new learnings about the benefits, risks, and challenges presented by evolving AI tools in use cases from healthcare and education to software development and cybersecurity.

A successful policy approach to AI will align with the following guidelines:

1. Harmonizing and Coordinating Approaches to AI

A wide range of federal, local, and state laws prohibit harmful conduct regardless of whether the use of AI is involved. For example, the Federal Trade Commission (FTC) Act prohibits a wide range of unfair or deceptive acts or practices, and states also have versions of these prohibitions in their statute books. The use of AI does not shield companies from these prohibitions. However, federal and state agencies alike must approach the applicability of these laws in AI contexts thoughtfully and with great sensitivity to the novel or evolving risks AI systems present. Congress and other policymakers must first understand how existing frameworks apply to activities involving AI to avoid creating sweeping new authorities or agencies that awkwardly or inconsistently overlap with current policy frameworks.

2. Quality Assurance and Oversight

Policy frameworks should utilize risk-based approaches to ensure that the use of AI aligns with any relevant recognized standards of safety, efficacy, and equity. Small software and device companies benefit from understanding the distribution of risk and liability in building, testing, and using AI tools. Policy frameworks addressing liability should ensure the appropriate distribution and mitigation of risk and liability. Specifically, those in the value chain with the ability to minimize risks based on their knowledge and ability to mitigate should have appropriate incentives to do so. Some recommended areas of focus include:

- Ensuring AI is safe, efficacious, and equitable.
- Encouraging AI developers to consistently utilize rigorous procedures and enabling them to document their methods and results.
- Encouraging those developing, offering, or testing AI systems intended for consumer use to provide truthful and easy-to-understand representations regarding intended use and risks that would be reasonably understood by those intended, as well as expected, to use the AI solution.

3. Thoughtful Design

Policy frameworks should encourage design of AI systems that are informed by real-world workflows, human-centered design and usability principles, and end-user needs. AI systems should facilitate a transition to changes in the delivery of goods and services that benefit consumers and businesses. The design, development, and success of AI should leverage collaboration and dialogue among users, AI technology developers, and other stakeholders to have all perspectives reflected in AI solutions.

4. Access and Affordability

Policy frameworks should enable products and services that involve AI systems to be accessible and affordable. Significant resources may be required to scale systems. Policymakers should also ensure that developers can build accessibility features into their AI-driven offerings and avoid policies that limit their accessibility options.

5. Research and Transparency

Policy frameworks should support and facilitate research and development of AI by prioritizing and providing sufficient funding while also maximizing innovators' and researchers' ability to collect and process data from a wide range of sources. Research on the costs and benefits of transparency in AI should also be a priority and involve collaboration among all affected stakeholders to develop a better understanding of how and under which circumstances transparency mandates would help address risks arising from the use of AI systems.

6. Modernized Privacy and Security Frameworks

The many new AI-driven uses for data, including sensitive personal information, raise privacy questions. They also offer the potential for more powerful and granular privacy controls for consumers. Accordingly, any policy framework should address the topics of privacy, consent, and modern technological capabilities as a part of the policy development process. Policy frameworks must be scalable and assure that an individual's data is properly protected, while also allowing the flow of information and responsible evolution of AI. A balanced framework should avoid undue barriers to data processing and collection while imposing reasonable data minimization, consent, and consumer rights frameworks.

7. Bias

The bias inherent in all data, as well as errors, will remain one of the more pressing issues with AI systems that utilize machine learning techniques in particular. Regulatory agencies should examine data provenance and bias issues present in the development and uses of AI solutions to ensure that bias in datasets does not result in harm to users or consumers of products or services involving AI, including through unlawful discrimination.

8. Ethics

The success of AI depends on ethical use. A policy framework must promote many of the existing and emerging ethical norms for broader adherence by AI technologists, innovators, computer scientists, and those who use such systems. Relevant ethical considerations include:

- Applying ethics to each phase of an AI system's life, from design to development to use.
- Maintaining consistency with international conventions on human rights.
- Prioritizing inclusivity such that AI solutions benefit consumers and are developed using data from across socioeconomic, age, gender, geographic origin, and other groupings.
- Reflect that AI tools may reveal extremely sensitive and private information about a user and ensure that laws require the protection of such information.

9. Education

Policy frameworks should support education for the advancement of AI, promote examples that demonstrate the success of AI, and encourage stakeholder engagements to keep frameworks responsive to emerging opportunities and challenges.

- Consumers should be educated as to the use of AI in the service(s) they are using.
- Academic education should include curriculum that will advance the understanding of and ability to use AI solutions.

10. Intellectual Property

The protection of intellectual property (IP) rights is critical to the evolution of AI. In developing approaches and frameworks for AI governance, policymakers should ensure that compliance measures and requirements do not undercut IP or trade secrets.