

May 28, 2024

Nancy La Vigne
Director
National Institute of Justice
810 7th Street NW
Washington, District of Columbia 20531

RE: Comments of ACT | The App Association, Request for Comments on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

In response to the Federal Register notice issued on April 25, 2024 (89 FR 31771), ACT | The App Association hereby submits comments to the National Institute of Justice (NIJ) to assist in the agency's research into the safe, secure, and trustworthy use of artificial intelligence (AI) in the criminal justice system.

The App Association represents small business innovators and startups in the software development and high-tech space located across the globe. App Association members create innovative software and hardware technology solutions and are at the forefront of incorporating AI into their products and processes.

Attached please find the App Association's general views on advancing governance, innovation, and risk management for government entity use of AI, including discussions of how to consider AI bias, ethical issues, and privacy and security of individuals' data. For any questions, please contact Chapin Gregor, policy counsel, at (202) 845-8814 or cgregor@actonline.org. The App Association appreciates the opportunity to provide comments to assist NIJ's work on these important matters.

Sincerely,



Brian Scarpelli
Senior Global Policy Counsel

Chapin Gregor
Policy Counsel

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

General Views of the App Association on Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence

The App Association represents small business innovators and startups in the software development and high-tech space located across the globe.¹ As the world embraces mobile technologies, our members create the innovative products and services that drive the global digital economy by improving workplace productivity, accelerating academic achievement, and helping people lead more efficient and healthier lives. Today, that digital economy is worth more than \$1.8 trillion annually and provides over 6.1 million American jobs.² App Association members create innovative software and hardware technology solutions and are at the forefront of incorporating artificial intelligence (AI) into their products and processes.

AI is an evolving constellation of technologies that enable computers to simulate elements of human thinking – learning and reasoning among them. An encompassing term, AI entails a range of approaches and technologies, such as machine learning (ML) and deep learning, where an algorithm based on the way neurons and synapses in the brain change due to exposure to new inputs, allowing independent or assisted decision making.

AI-driven algorithmic decision tools and predictive analytics are having, and will continue to have, substantial direct and indirect effects on Americans. Some forms of AI are already in use 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 forward, across use cases and sectors, AI has incredible potential to improve American consumers' lives through faster and better-informed decision making enabled by cutting-edge distributed cloud computing. As an 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. AI will also play an essential role in self-driving vehicles and could drastically reduce roadway deaths and injuries. From a governance perspective, AI solutions will derive greater insights from infrastructure and support efficient budgeting decisions.

¹ ACT | The App Association, *About*, available at <http://actonline.org/about>.

² ACT | The App Association, *State of the U.S. App Economy: 2023*, <https://actonline.org/wp-content/uploads/APP-Economy-Report-FINAL-1.pdf>

Today, Americans encounter 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 (we urge consideration of these forms of AI as “narrow” AI). The App Association notes that this “narrow” AI already provides great societal benefit. For example, AI-driven software products and services revolutionized the ability of countless Americans with disabilities to achieve experiences in their lives far closer to the experiences of those without disabilities.

Nonetheless, AI also has the potential to raise a variety of unique considerations for policymakers. The App Association appreciates the efforts to develop a policy approach to AI that will bring its benefits to all, balanced with necessary safeguards to protect consumers.

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. 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.

6. 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.

7. 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.

In addition, government entities should avoid requirements that may have the effect of eroding end-to-end encryption in AI-powered services. The potential erosion of end-to-end encryption could create a disproportionate advantage for larger entities with the resources to comply with new regulations while maintaining user trust. Meanwhile, smaller businesses might struggle to navigate the trade-offs between compliance and maintaining their competitive edge based on privacy and security. In this regard, small app companies' interests are aligned with those of end users and children, who benefit immensely from the protections end-to-end encryption. The goal of facilitating investigation and content filtering must be weighed against the twin imperatives of empowering people to benefit from end-to-end encryption and fostering an environment conducive to innovation and growth. Sacrificing these latter aims in service of the former would result in a reduction in online safety for minors; undermined privacy and security protections for consumers, leading to undue financial and reputational harms; and weaker business prospects for small business innovators.

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 safeguards for IP or trade secrets.