Request for Information to the Update of the National Artificial Intelligence Research and Development Strategic Plan: Responses

Pangiam

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government or any entity within the U.S. Government. We bear no responsibility for the accuracy, legality, or content of the responses and external links included in this document.
March 4, 2022

Office of Science and Technology Policy
The White House
1600 Pennsylvania Ave NW
Washington, DC 20500

RE: RFI Response: Update of the National Artificial Intelligence Research and Development Strategic Plan

Mapping to the strategic plan point, “Develop Shared Public Datasets and Environments for AI Training and Testing,” Pangiam offers the following response to the Office of Science and Technology Policy’s (OSTP) request for information, “Update of the National Artificial Intelligence Research and Development Strategic. Pangiam is a national security software and technology company applying computer vision to define the future of trusted movement and security. We are revolutionizing the future of operations, security, and safety at airports, seaports, and land crossings as well as on air force bases using emerging technologies. Our technology and expertise in computer vision and artificial intelligence (AI) is recognized by the National Institute of Standards and Technology (NIST). Our facial recognition algorithm recently achieved a top three ranking in the NIST Face Recognition Vendor Test 1:N Identification and is ranked the fastest in the world by NIST’s most recent 1:1 test.

We are also experts at deploying biometric technology for identity verification in a variety of trade and travel use cases, working in partnership with private sector entities and

---

1 OSTP, Request for Information to the Update of the National Artificial Intelligence Research and Development Strategic Plan, 87 FR 5876 (February 2, 2022).
government. In the private sector, Pangiam’s technology is trusted and used by the departure control system of over thirty-five airlines. For government, Pangiam developed the U.S. Customs and Border Protection’s cloud-based facial biometric matching service, known as the Traveler Verification Service. In a collaborative effort, Pangiam is the technology provider that enables a partnership between Delta Air Lines and the U.S. Transportation Security Administration for their digital ID program.

Pangiam employs an industry-leading rigorous governance program to ensure the accuracy, efficiency, and security of our technology and build trust with clients and the users of our technology. Our company has expended private resources to develop artificial intelligence algorithms with the highest ethical standards. As federal entities like OSTP and the National Artificial Intelligence Initiative Office consider policies to support U.S. AI research and development (R&D), we propose two key recommendations to ensure the ethical advancement and use of biometric and AI technology and to keep the United States competitive edge with international competitors. Our first recommendation is to provide private companies access to government datasets to train their algorithms and, second, for the U.S. government to leverage technical safeguards and policy incentives to ensure ethical AI development by the private sector.

Beyond developing and deploying AI for identity verification, Pangiam has partnered with Google Cloud to further automate threat detection at passenger screening checkpoints using AI. This solution, named Project DARTMOUTH, allows for better detection of prohibited items, and introduces a new capability of aggregated threat detection for complex, coordinated threats across screening lanes, checkpoints, and airports. This technologic development,
however, has outpaced the United States’ capability to acquire and deploy it. While already in pilot in the UK, there are legal, policy, and operational barriers regarding the use of AI by federal entities that need to be addressed to be able to leverage this capability. To overcome these barriers, we recommend that the forthcoming update to the National AI Research and Development Strategic Plan include research into the legal, policy, and operational impacts of AI on federal agencies.

**Artificial Intelligence in Identity Verification**

The use of AI for identity verification in the trade and travel domain offers several key benefits to create operational efficiencies, increase the security and safety of air travel, and improves the traveler experience. Biometric identity verification automates manual human processes which reduces labor costs and errors caused by fatigue. This automation verifies passenger identity more quickly than manual processes, cutting time for processes like boarding almost in half, reducing potentially costly late departures, and allowing for growth of aviation operations within existing infrastructure constraints.²

Identity verification in travel is the cornerstone of aviation security. Using biometric technology to verify a passenger’s identity increases the security of travel as algorithms outperform humans in identifying imposters.³ From a safety perspective, at several points in a passenger journey the passenger physically exchanges documents to verify their identity.

Biometric identity verification is contactless, reducing the potential points of transmission for viruses and enabling physical distancing at otherwise crowded chokepoints.

Our use case is narrow, explicitly used to facilitate the movement of people and goods. Despite this narrow application, there are still instances in which the companies developing this technology could cause harm. First, is in the development of AI algorithms. The size and quality of datasets used to train algorithms could cause disparity in performance across different demographics. Without high performance across all demographics, the facilitation and efficiency benefits for large, diverse populations such as the traveling public are lost.

Second, it is costly and time consuming to acquire large and diverse datasets, which has led some organizations to blur and cross ethical and legal lines in acquiring them. Additionally, poor data security and data protection practices can leave biometric information vulnerable to nation-states, hackers, or even the highest bidder through third party sales. In a recent example, one company improperly harvested customer data through deceptive methods, training its algorithm on a consumer-facing application designed to acquire dataset images without informing the consumer. Further, consumer data was retained indefinitely even after accounts were deactivated. This is just one example, but many more exist and will continue to so long as these datasets remain a barrier to development.

Access to and Ethical Safeguards for Datasets

Pangiam has proactively adopted its own Biometrics Principles to fully realize the benefits and neutralize the potential harms of this rapidly advancing technology. From data sourcing and acquisition to deployment, Pangiam’s industry-leading principles protect the
integrity of the technology and process against malfeasance and abuse. While our company has adopted this policy voluntarily, if not properly regulated, biometric technology has, like all technologies, the potential to be misused. If the United States is to maintain its lead in trustworthy AI R&D, it must promote the adoption of rigorous ethical behavior for AI research in the private sector.

U.S. federal initiatives and policymaking to promote this ethical behavior must start with how algorithms are developed. In this first stage, private companies must acquire or create datasets for algorithms to be trained on. This is a costly, time-consuming step that has already led to many examples of unethical shortcuts in the industry, breaching legal agreements and eroding the confidence of the American public in AI. Access to government biometric datasets would speed the development of trustworthy U.S. algorithms, leapfrogging U.S. companies past this initial barrier to development.

Internationally, governments are already sharing their datasets with their private sector to help advance AI performance. In our closest competitors, this sharing is a key reason for the rapid advancement of their capabilities, but few, if any, ethical guardrails are required for companies to access to billions of images. In the United States, access to government datasets can be done in an ethical fashion with technical safeguards and policy incentives. Technical safeguards, such as training algorithms behind a firewall, can ensure companies only have access to results rather than the underlying data. Policy incentives, such as requiring ethical corporate behavior either by audit, pledge, or other disclosure and no past abuse of consumer data, can ensure that only responsible companies that abide by an ethical code of conduct can take advantage of this resource.
The U.S. government is already sharing data with the private sector for AI development. The National Geospatial-Intelligence Agency (NGA) shares geospatial data with the private sector to help the agency solve some of its current AI challenges and employing advanced algorithms. NGA takes its engagement with the private sector a step further and runs an accelerator to grow the number of advanced solutions available to NGA. The Pentagon’s Joint Artificial Intelligence Center uses the Joint Common Foundation, a cloud-based platform that enables users to access Defense Department data and develop AI solutions in a secure environment. These are just two examples, but there are more that could be leveraged as a model for sharing datasets with the private sector for training facial recognition algorithms.

The U.S. government has a responsibility to its citizens to ensure the ethical development and use of AI. Federal agencies have their own requirements for data access, but facial recognition requires the highest ethical corporate behavior. Pangiam offers the following principles for consideration as ethical requirements for U.S. companies to access federal datasets for AI R&D for facial recognition.

- **Data Transparency.** Regularly and publicly communicate how information is stored, transmitted, and accessed, and the privacy policies governing biometrics use simplified, easy to understand language.

- **Opt-In Databases.** Travelers to affirmatively opt-in to biometric collection.

- **Opt-Out Operations.** Areas where biometrics are captured are clear and obvious and an operational policy for those who opt-out is deployed.

- **Privacy-by-Design.** Systems are designed and implemented that protect the privacy of the traveler.

- **Security Safeguards.** Use encryption and biometric algorithms whose face templates cannot be reverse engineered to identify a traveler.
- **Performance and Accuracy.** Use only biometric algorithms that have the highest rates of accuracy and precision as determined by The National Institute of Standards and Technology.

- **Domestic Development.** Algorithms are developed in the United States.

- **Ethically sourced Datasets.** Datasets are ethically and legally sourced and contain a wide range of demographics to reduce bias.

- **No Third-Party Sales.** Prohibit the sale of biometric and biographic information to third parties; and

- **A Track Record of Trust.** Organizations that are known or found to have abused customer privacy, misled consumers, or insufficiently protected data are excluded from accessing government datasets.

While ethical behavior by the private sector is paramount to developing trustworthy AI in the United States, any federal effort to verify the desired corporate behavior must keep in mind the speed at which biometric technology is being developed worldwide. In order to maintain a competitive edge against global competitors, this ethical verification effort cannot be so cumbersome for the private sector as to inhibit innovation and therefore counterproductive to the United States’ overall aim at leading AI R&D. In the same vein, any technical safeguards must not be so complex as to prohibit the ability of an ethically verified company to use the dataset.

Beyond incentivizing ethical behavior, access to government datasets would address a key cause of inconsistent performance across different demographic groups or “algorithmic bias.” There is an overrepresentation of Caucasian images in many public and private datasets and, when algorithms are trained on datasets that lack diversity, it leads to bias in facial matching of underrepresented groups. Pangiam is committed to eliminating bias in its facial recognition models and we already strive to train our models on datasets that have equal
representation across gender and ethnicity. We do this because of our strong ethical principles, and this diligence results in better parity of performance across demographic groups. The U.S. government can help the private sector writ large produce higher performing models with access to diverse government datasets.

**AI Enablement Beyond Research and Development**

In mid-2020, airport operators, regulators, control authorities and industry bodies from around the globe, including the United States, endorsed an Open Architecture policy for airport security systems. This policy was a paradigm shift in transportation security, decoupling original equipment manufacturers from the software used on transportation security equipment. Removing vendor lock-in on detection algorithms opened the door for non-traditional software developers to enter the transportation security market. Third-party threat detection AI algorithm developers quickly demonstrated interest and capability in this opportunity.

These new entrants provide a full generational leap forward in AI use for threat detection technology, allowing for better detection of prohibited items, more advanced detection capabilities, and reducing false alarms. More advanced threat detection capabilities, known as aggregated threat detection, can detect complex, coordinated threats across lanes, checkpoints, and even airports, all while maintaining consistently high checkpoint throughput numbers. While U.S. support was a key factor in the Open Architecture policy successfully encouraging AI R&D in transportation security, there are non-technology barriers to the United States benefitting from this achievement.

---

There is a misconception that AI R&D is a purely technologic concern. The development of AI for threat detection has revealed, however, that many barriers to its deployment are not in R&D, but in support and policy functions. Therefore, any strategic plan to advance AI R&D include understanding the impact of AI on enterprise and operational support functions. AI R&D will result in legal, policy, and operational issues in almost all federal agencies. The federal government will need to review its own internal policy and processes to ensure readiness to enable the acquisition, deployment, and regulation of this technology. AI R&D is moving quickly, and these ancillary functions must not be overlooked in the forthcoming strategy update if the United States is to maintain leadership in AI R&D.

Pangiam welcomes the opportunity to participate in further discussions to ensure that AI R&D is conducted ethically and enables the United States to maintain its global competitive advantage. We are also willing to share insights on non-R&D opportunities for the federal government to enable development of this technology.

Respectfully submitted,

Shaun Moore
Chief Artificial Intelligence Officer
Pangiam
7950 Jones Branch Drive
McLean, VA 22102