Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.
January 15, 2022

Dr Eric Lander, The President’s Science Advisor and Director of OSTP
Dr Alondra Nelson, OSTP Deputy Director for Science & Society
Office of Science and Technology Policy
The White House
1600 Pennsylvania Ave NW
Washington, DC 20500
Via email to: BiometricRFI@ostp.gov

Dear Dr Lander and Dr Nelson,

**Microsoft Response to OSTP Request for Information on Public and Private Sector Uses of Biometric Technologies [Document Number: 2021-21975]**

Microsoft appreciates the opportunity to provide feedback in response to the Office of Science and Technology Policy’s Request for Information on Public and Private Sector Uses of Biometric Technologies as part of its initiative to develop a Bill of Rights for an Automated Society. We share OSTP’s view that AI and other data-driven technologies must serve society equitably and respect the enduring values of American democracy. Through policy, process, and technological measures, we need to harness the beneficial uses of AI technologies and mitigate their potential misuse and harms. OSTP’s Bill of Rights initiative is a timely and important contribution to the discussion of what effective guardrails ought to look like, and we look forward to sharing our knowledge and experiences in support of the initiative.

**Facial Recognition Technology: An Instructive Case Study**

Since 2018, Microsoft has engaged in an expansive program of work to better understand the sociotechnical implications of facial recognition technology, and to design and enact effective safeguards to harness its benefits and guard against its potential risks. This work has been conducted in partnership with experts inside and outside of the company, and has included the development of legislative proposals¹ as well as the internal adoption and implementation of Facial Recognition Principles.² We have found the work to be instructive not just for ensuring the safe and rights-respecting use of facial recognition technology, but for our responsible AI program more generally.³ Below, we set out some key insights in the spirit of sharing our lessons learned and helping inform OSTP’s initiative.

---

³ We describe key elements of our governance program below; *see also* Natasha Crampton, *The Building Blocks of Microsoft’s Responsible AI Program*, Microsoft (Jan. 19, 2021), [https://blogs.microsoft.com/on-the-issues/2021/01/19/microsoft-responsible-ai-program/](https://blogs.microsoft.com/on-the-issues/2021/01/19/microsoft-responsible-ai-program/).
Centering on use cases and calibrating risk and mitigations

Facial recognition systems can create risks that are sociotechnical in nature—they arise at the intersection of technology and society and are highly sensitive to the context of use. Specifically, three categories of risk often rise to the top of discussions about facial recognition systems: risks of bias and discrimination, the potential for new intrusions on privacy, and possible threats to democratic freedoms and human rights. When and how those potential risks materialize, who they may impact, and how evenly they are distributed is highly dependent on the use case for the technology. For example, using facial recognition technology to unlock a device has very different implications than using it for ongoing surveillance in a law enforcement context. As a result, we appreciate and endorse OSTP’s commitment to an assessment of use cases that is finely tuned and granular.

Beyond the specific use case for an AI system, it is important to study other factors that influence its overall risk profile. AI systems vary widely in their degree of automation, the readiness of the technology for the application, and the complexity of the deployment environment. Therefore, Microsoft believes that any regulatory framework or principles should take a risk-based approach. We encourage OSTP to draw upon the work led by NIST to define an AI Risk Management Framework. We support NIST’s commitment to adopt an approach that is flexible, outcomes-based, and designed to secure positive influences of AI systems while minimizing their potential negative impacts.

Conducting impact assessments

Impact assessments can play an important role in identifying and mitigating the sociotechnical risks of specific AI deployments. At Microsoft, completing an impact assessment is the first step in our Responsible AI by Design process. Assessments are conducted by multi-disciplinary teams, which include product managers, data scientists, designers, and product counsel, and with the benefit of input from user research. By interrogating a system’s purpose, stakeholders, intended uses, deployment geographies, and failure modes, among other things, assessment teams gain a deeper understanding of the impact of their AI systems and how to design effective mitigations for potential harms. Further, Microsoft uses the outcomes of individual assessments to inform other product cycles: many common mitigations and effective strategies have been incorporated into our Responsible AI Standard as standard product development requirements for AI systems. These standard procedures include a structured process to identify, measure, and mitigate potential fairness-related harms of AI systems, and requirements to establish feedback channels and ongoing evaluation procedures.

---

4 For example, the Partnership on AI has produced a helpful paper explaining how different types of facial recognition systems work. This paper was the result of a series of workshops on facial recognition systems convened by PAI between September 2019 and January 2020. It brought together Partner organizations and communities developing, engaging with, and affected by these systems. Partnership on AI, Understanding Facial Recognition Systems (2020), http://partnershiponai.org/wp-content/uploads/2021/08/Understanding-Facial-Recognition-Paper_final.pdf.


7 We focus on three types of fairness harms: quality of service, allocation harms, and representational harms.
Facilitating the responsible use of facial recognition technology

In addition to proactive harm mitigation, we encourage our teams to engage in systems-level thinking about the technology they are developing. This thinking keeps people at the center of AI systems and highlights additional steps necessary to facilitate responsible deployments by our customers.

Microsoft makes its facial recognition technology available through cloud-based application program interfaces (APIs) that can be called by our customers. In this model, our facial recognition API, Face API, is a building block that our customers use to create a facial recognition system. A facial recognition system includes the technology as well as the people who will use it, the people who will be subject to it, and the environment in which it is deployed. To be fit for purpose, the facial recognition system must be both a valid solution to the problem it is intended to solve and a system that warrants trust by individuals and society.

Compared to more traditional forms of software development, creating an AI system that is fit for purpose requires greater knowledge transfer between developers of the technology and deployers of the system. This is because decisions about how to deploy a system, including the societal context in which it is used, have a significant impact on any potential risks the system may generate. As such, it is important that deployers have the information needed to make responsible deployment decisions and identify and address any potential risks. Through our facial recognition work, we have developed effective mechanisms and channels for information transfer between developer and deployer. In particular, our Face API Transparency Note communicates—in understandable language aimed at non-technical audiences—how Face API works, the choices deployers can make that influence accuracy, and the importance of thinking about the whole system during deployment. The Note also clearly explains the importance of keeping a human in the loop for deployments of Face API. This type of stakeholder communication is an important practice to secure the responsible deployment of the technology.

Developers must go beyond creating technologies that meet needs and social expectations and ensure that AI systems are tested to ensure their deployments take into consideration safety concerns, as well as concerns of individual rights and those around democratic norms. Microsoft believes that it is incumbent on developers to not just undertake their own testing prior to releasing technology, but also to facilitate testing by independent third parties and participate in established benchmark testing programs such as NIST’s Ongoing Face Recognition Vendor Test. While there are some respects in which NIST’s tests would benefit from modernization and refinement, benchmark testing is important to enable comparisons across vendors and develop an understanding of the state-of-the-art of the technology. However, as with all testing, benchmark tests only indicate how the technology will work in conditions that reflect the benchmark data, and there will always be limits on the number of conditions that benchmark testing programs can model. This then leads to the critical need for operational testing, by which we mean testing by deploying entities in the context in which the system will be used and with the people who will interact with the system. Microsoft provides guidance on specific considerations for conducting operational testing in the “Plan for an evaluation phase” section of our Face API Transparency Note. This includes information about the importance of collecting ground truth data.

evaluation data, considering factors such as sensor position and lighting, and seeking feedback from the people who are operating the system and those who are impacted by the system.

Common uses of facial recognition technology
Customers use Microsoft’s facial recognition technology in a wide range of applications. Set out below are some common uses of facial recognition technology that we believe can be deployed with known, effective safeguards like those that Microsoft has implemented through its Facial Recognition Principles. We also believe that these safeguards can be included in new regulations and laws, further described in the next section.

- **Facial Verification to Access Secured Devices and Services.** Face API is frequently used to verify a person’s identity to grant them access to secured devices and services, for example by matching a selfie against another photo on file to prove identity and enable a product or service. National Australia Bank, for example, has experimented with using Microsoft’s facial verification technology to allow customers to withdraw money from an automated teller machine without using a bank card.⁹

- **Touchless Access Control.** Face API is often used to enable enhanced touchless access experiences. With appropriately trained human supervision, facial recognition can help individuals complete check-in processes at airports, stadiums, theme parks, and other high-traffic areas. In addition to speeding up the process and reducing the burden of producing a physical method of authentication, facial recognition technology minimizes the risks posed to hygiene and security from the loss or theft of physical methods of authentication such as credit cards or tickets.

- **Personalization.** Face API can be used to enable ambient personalization and enrich experiences on shared devices. For example, where meaningful explicit consent experiences are implemented, devices that know an individual, such as home computers and work kiosks, can recognize those individuals and provide personalized services, such as hands-free interaction or directions to a meeting. These deployments also assist individuals with dyslexia and other disabilities for whom character input requirements (i.e., passwords) may be burdensome.

- **Enable Accessibility.** Microsoft projects, such as Seeing AI¹⁰ and Project Tokyo,¹¹ use facial recognition technology to provide more immersive social experiences for people who are blind or low vision.

---


- **Digital Access and Cybersecurity.** According to a recent Government Accountability Office report, sixteen U.S. federal agencies rely on facial recognition technology for digital access or cybersecurity. Uses range from unlocking devices with facial recognition to identity verification of individuals using government websites. These authentication tools are important assets to prevent cybercrime and other malicious actions taken on digital devices.

- **Law Enforcement.** Law enforcement agencies use facial recognition technology for a range of use cases, including identification of victims of crime, missing persons, and other investigative efforts. While Microsoft believes that certain use cases can support the public interest if guided by appropriate legislative guardrails like those outlined in the section below, we also recognize that the United States has a strong need for a whole-of-society conversation about how the police should—and should not—use facial recognition technology. In 2020, as the nation’s attention turned to issues at the intersection of racial equity and policing, Microsoft affirmed our policy position that we will not sell facial recognition to police departments in the United States until a strong law, grounded in human rights, has been enacted. It is our hope that this position will help create space for the much-needed societal conversation about the use of advanced technologies, such as facial recognition, in policing.

**New Laws Are Needed, and Effective Safeguards Have Been Identified**

While Microsoft will continue to uphold our Facial Recognition Principles and exercise restraint in decisions about the design, development, and deployment of our technology, we remain convinced that regulation of facial recognition technology is essential and time sensitive. In particular, we need strong laws grounded in human rights to provide people with protection under the law and avoid a commercial race to the bottom. Our position on regulation is informed by our internal work developing company-wide Facial Recognition Principles, implementing those principles through our internal governance program, and our external engagement with customers, partners, civil society organizations, academics, and policymakers. We believe there are specific, effective safeguards that can be adopted now to establish the right guardrails for the beneficial use of the technology. For facial recognition systems deployed by government agencies, these safeguards include:

- Upfront transparency and accountability measures, such as a requirement for government agencies to adopt a publicly available facial recognition policy in advance of system implementation and to consult impacted communities on a regular basis before and after adoption.
- Requirements to only use technology that is testable by independent third parties (e.g., via an API) and subject to benchmark and operational testing on a regular basis.
- Requirements to train employees using facial recognition systems and carry out meaningful human review of decisions that impact legal rights or have similarly significant impacts on individuals.

---

• Due process protections and record-keeping requirements, including pre-trial disclosure of the use of facial recognition technology to criminal defendants, and statutory reporting obligations akin to those imposed in the Wiretap Act.

• Restrictions on certain use cases, including:
  o A prohibition on the use of facial recognition technology for indiscriminate, mass surveillance.
  o Restrictions on the use of facial recognition to engage in targeted ongoing surveillance of specific individuals. Such use should only occur when it would provide evidence of a serious criminal offense, and when either a search warrant has been obtained or there are exigent circumstances (i.e., immediate danger of death or serious physical injury to any person).
  o A prohibition on the use of facial recognition in a manner that could discriminate based on protected characteristics, chill First Amendment activities, or otherwise infringe on human or constitutional rights.

Many of these protections have been adopted in Washington State’s facial recognition law, which is the first law of its kind to enact specific legal guardrails on the use of facial recognition technology by government agencies. Like most initial forays into a new legal field, the Washington law can be improved upon and will evolve with experience in the future; however, it remains an important initial articulation of safeguards that should attend government use of facial recognition technology.

Additional regulatory safeguards for commercial use cases should include:

• Requirements for commercial facial recognition service providers to:
  o build technology that is testable by independent third parties (e.g., via an API) and to implement mitigation plans in the event that independent testing reveals material unfair performance differences across demographic groups;
  o provide documentation that explains the capabilities and limitations of the technology in terms that deploying organizations and consumers can understand, and that enables deploying organizations to conduct operational testing; and
  o contractually prohibit the use of their services to unlawfully discriminate.

• Requirements for organizations deploying facial recognition technology to:
  o ensure testing in operational conditions and implementation of reasonable guidance from developers to ensure best quality results;
  o provide conspicuous and accessible notice of all uses of facial recognition technology;
  o secure explicit consent for all persistent tracking, identification, or verification tasks except in narrow security scenarios that conform to strict limits.

• Restrictions on private sector disclosures to law enforcement agencies of face templates or other personal data derived from facial recognition technology, unless such disclosure is with the consent of the individual concerned, required by law, or necessary to respond to an emergency involving danger of death or serious physical injury to any person.

In addition to the safeguards set out above, the responsible deployment of facial recognition systems in commercial settings would be strengthened in important ways by the protections afforded by a comprehensive federal privacy law.

**Governance as a Strong Foundation for Building AI Systems that Warrant Trust**

Microsoft believes that a strong internal governance program is necessary to enact principled commitments to responsible AI and support the ongoing evolution of policies and practices that is necessary in this complex, fast-moving domain. Our approach is research-led, governed by policy, and supported by engineering systems and tools. It embraces the “hub-and-spoke” model that has worked successfully to integrate privacy, security, and accessibility into our products and services.

Our “hub” includes: the Aether Committee, whose working groups leverage top scientific and engineering talent to provide subject-matter expertise on the state-of-the-art and emerging trends regarding the enactment of Microsoft’s AI principles; the Office of Responsible AI, which sets our policies and governance processes; and our Responsible AI Strategy in Engineering (RAISE) group, which enables our engineering groups to implement our responsible AI processes through systems and tools. The three groups work together to set a consistent bar for responsible AI across the company and they empower our “spokes” to drive initiatives and be accountable for them.

The spokes of our governance include our Responsible AI Champs community. The Champs are appointed by company leadership and sit in engineering and sales teams across the company. They raise awareness about Microsoft’s approach to responsible AI and the tools and processes available, they spot issues and help teams assess ethical and societal considerations, and they cultivate a culture of responsible innovation in their teams.

To enact our principled commitment to responsible AI, we have developed our Responsible AI Standard, an internal set of product development rules that sets out how we enact our AI principles and that is underpinned by Microsoft’s corporate policy. Now in its second version, the Responsible AI Standard recognizes the need to actively guide a process of Responsible AI by Design, including through practices such as impact assessments and fairness testing. We are engaged in the process of systematically rolling out the Responsible AI Standard across the company and building the set of implementation methods that teams can draw upon, including tools, patterns, and practices crowdsourced from within and outside the company and refined through a maturity process.

We have also established a process for ongoing review and oversight of high-impact cases and rising issues and questions, since we recognize that high-impact cases warrant additional oversight, and it is impossible to reduce all the complex sociotechnical considerations into an exhaustive set of pre-defined rules. Our Sensitive Uses process requires that use cases that meet our review criteria are reported to our Office of Responsible AI for triage and review, which includes a deliberation when there is no existing precedent to draw upon. Since July 2019, we’ve processed over two hundred use case reviews, including an uptick in reviews since March 2020 as more Microsoft teams and customers sought to use AI technologies amid applications and opportunities with harnessing data and AI methods to mitigate challenges with Covid-19.
We have also been engaged in work to build out the “paved road” for responsible AI at Microsoft – the set of tools, patterns and practices that help our engineering teams easily integrate responsible AI requirements into their everyday development practices. Although tooling – particularly in its most technical sense – is not capable of the deep, human-centered thinking work that needs to be undertaken while conceiving AI systems, we think it is important to develop repeatable tools, patterns, and practices where possible so the creative thought of our engineering teams can be directed toward the most novel and unique challenges, not reinventing the wheel. Integrated systems and tools also help drive consistency and ensure that responsible AI is part of the everyday way in which our engineering teams work. Our AI development platform, AzureML, serves as the foundation for this paved road, so that our customers will also benefit from our development of engineering systems and tools. Our Responsible AI Dashboard is our most recent release: it’s a single pane of glass that brings together several mature responsible AI tools in the areas of machine learning interpretability, unfairness assessment and mitigation, error analysis, causal inference, and counterfactual analysis. This helps developers undertake holistic assessment and debugging of models and is the product of deep research-to-practice collaborations between our Aether community and engineering teams over several years.

Key Considerations for Effective AI Policymaking
Microsoft believes that policymaking for AI generally and facial recognition technology specifically must be approached with a deep understanding of the technology and its use cases as well as a clear understanding of the problems regulation seeks to solve. Answering these questions will require broad input from stakeholders who develop, deploy, or are impacted by AI systems. OSTP has begun this discussion thoughtfully in the current RFI and its other consultation initiatives. In addition, AI regulation will need to fit into existing laws and regulatory schemes: gaps and areas for improvement should be identified before proceeding. To this end, Microsoft endorses a review of the adequacy of existing civil rights enforcement authorities as recommended by the BSA | The Software Alliance in its RFI response of January 13, 2022. Finally, we believe that government, industry, civil society organizations, and other stakeholders must be agile when working to secure rights-respecting outcomes in a complex, fast-moving domain; this will likely require an incremental approach to policymaking.

Conclusion
Microsoft appreciates the opportunity to contribute its learnings from its facial recognition and governance efforts and welcomes further dialogue on these topics as OSTP progresses its Bill of Rights initiative. We stand ready to assist OSTP in shaping the guardrails to ensure that AI and other data-driven technologies serve society equitably and respect the enduring values of American democracy.

Sincerely,

Natasha Crampton
Chief Responsible AI Officer
Microsoft Corporation