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.
Biometrics are based on good science. However, like any other science, there are limitations to how the science is applied. In order to understand and characterize the limitations of biometrics as a science and in specific applications, it is critical that the system is decomposed into its constituent parts and each part is well-described analytically.

Biometrics as a class of technologies is not inherently an AI-embedded class of technologies. Biometrics existed long before Artificial Intelligence (AI) or even computers existed; e.g., fingerprinting as a forensic science has been used extensively since the 1880s. In many ways, more importantly, humans have used biometrics (e.g., face, voice, and gate) since the beginning of recorded history. The way the human brain recognizes other humans has influenced our understanding of biometrics for many years. It is important to note that biometric applications do not operate the same way that the human brain operates. Furthermore, the portrayal of biometrics through media and entertainment is often inconsistent with the realities of the technologies.

A number of biometric systems do use AI algorithms, and this is an artifact of the fact that AI algorithms are well suited for many classes of image processing, and that image processing is a key part of some kinds of biometrics, including voice recognition systems.

Because of the complexities of AI systems, they often produce matching or other decision results that are not easily understood by humans interpreting the outputs. Consequently, the development of explainable AI is a high priority for a number of government agencies including the Department of Defense. Biometric applications of AI are explainable, and every effort should be made to maximize operational explanations of how exactly biometric systems work. Further, intellectual property rights and considerations are sometimes limiting factors in biometric algorithm expandability. IP rights and expandability should be major considerations in the development of governance. Biometrics are used extensively across government and industry. In order to correctly make policy in regards to the use of biometrics, it is important to understand the key elements of biometric systems and how the different parts of the system contribute to the
performance of the system. The key components of biometrics as a science and as a technology are the following:

**Biological differences:** Each human has specific biological characteristics that are created through random developmental processes (e.g., irises and fingerprints), heredity (e.g., DNA), and other factors. What is important is the amount of information the biology provides to the system. Some biological indicators have a lot more information than others and some are more consistent than others. For example, DNA is both data rich and very consistent. Face recognition has less data and is less consistent.

**Feature definition:** Feature definition is a technical process that takes the biological indicators and converts them into computable data that can be input into matching algorithms.

**Matching algorithms:** The matching algorithms are used to determine an identification match. Neither feature definition nor matching algorithms are perfect and have some degree of accuracy issues.

**Manual verification:** Many implementations of biometric systems are computer-aided applications. That is, the computer makes recommendations to a human operator who then makes final decisions about matches. This is common in law enforcement and national security applications. Performance of man-in-the-loop systems can suffer from accuracy issues for both the computer systems and the human operators.

**Specific application:** Lastly, the specific application has a lot to do with the reliability and accuracy of any biometric system. Small changes in how a biometric system operates can radically change its reliability, performance, and intrusiveness.

**National Defense and law enforcement applications** It is important to note that in the 21st century, the use of biometric systems is critical to achieving and maintaining national defense and rule of law at its current rate of effectiveness. The loss of this technology as a tool for national defense and law enforcement would have significant impacts to the safety of the United States. It is clear that the adversaries of the United States and our international competitors will not limit the use of biometrics for their own national security in any meaningful way.

Given the complexity of biometrics and their criticality to national security and rule of law, it is required to ensure that policy decisions are informed by technical experts and by a clear understanding of the specifics of the applications. As a result, decisions about the use of biometric technology should be made in direct consultation with engineers and other technical experts with a deep understanding of the technology.

1. **Descriptions of use of biometric information for recognition and inference:** Information about planned, developed, or deployed uses of biometric information, including where possible any relevant dimensions of the context in which the information is being used or may be used, any stated goals of use, the nature and source of the data used, the deployment status (e.g., past, current, or planned deployment) and, if applicable, the impacted communities.
Comments:

a) The use of traditional biometrics for identification and verification of identity to control access and enforce security will continue to grow in both the national security and commercial application spaces.

b) The traditional application of biometrics for surveillance will grow in the commercial sector as companies recognize the value of data on people movement.

c) In the past few years the technology has advanced to a point where the use of biometrics for inference is reliable and cost effective to a point where it is viable for commercial applications. This data can and will be used for both customization of services and for customization of influence. We can expect that industry will grow its use of biometric technology for inference significantly in the next 10 years. The data collected for inferencing can and will be used by a variety of Artificial Intelligence algorithms to influence people in using marketing and other influencing methods (targeted presentation of data) in a highly individualized and targeted manner.

2. Procedures for and results of data-driven and scientific validation of biometric technologies: Information about planned or in-use validation procedures and resulting validation outcomes for biometric technologies designed to ensure that the system outcomes are scientifically valid, including specific measures of validity and accuracy, resulting error rates, and descriptions of the specific measurement setup and data used for validation. Information on user experience research, impact assessment, or other evaluation of the efficacy of biometric technologies when deployed in a specific societal context is also welcome.

Comments:

a) Validation of the performance of biometric systems and their use in an ethical manner are both important and required to protect the rights of people and the availability of biometric systems to law enforcement and national security applications.

b) The use of AI and other non-linear algorithmic methods as well as the very large data sets that are often used in the development and operations of biometric systems makes these systems very difficult to test completely. As noted in many studies and earlier in this response, the complexities of biometrics require us to look at and validate more than just the aspects of biometric systems. Complete verification and validation require: i) validating the performance of the science and algorithms, ii) validating the design and application of biometrics to a specific system or purpose, and iii) validating the risks and benefits of that systems in their intended use.

c) Currently, the most complete testing of biometric testing being conducted is being done by NIST, the National Institute of Science and Technology. This testing should continue and be expanded to increase its usefulness across technologies, modalities, and applications.

d) Currently the Department of Defense has a very robust model for the development and execution of developmental and operational testing. There are processes used to ensure the performance and safety on weapons used by the military that could also be used as a model for an independent test agency to define and conduct testing of both government and commercial biometric applications.
e) Finally, a risk-based, comprehensive method for biometrics benefits analysis needs to be created and administrated by an engineering and science-based government or non-profit organization to ensure that promised benefits are achieved and risks and harms investigated and mitigated across the multitude of biometric techniques and their use in combination with one another.

3. **Security considerations associated with a particular biometric technology**: Information about validation of the security of a biometric technology, or known vulnerabilities (such as spoofing or access breaches). Information on exhibited or potential leaks of personally identifying information via the exploitation of the biometric technology, its vulnerabilities, or changes to the context in which it is used. Information on security safeguards that have been proven to be efficacious for stakeholders including industry, researchers, end users, and impacted communities.

**Comments:**

a) Biometric security systems and the securing of biometric input signals and images from cyber-attacks have the same issues as any computer system. Like any other computer-based system, appropriate levels of cyber security protection need to be put in place for any biometric system.

b) Much has been made of potential issues with the loss or compromise of biometric images and or biometric templates. It has been said that, unlike passwords, a person only has one set of fingerprints, and only one face, and once the template is compromised it is a significant security issue. Although this is very much true, current methods for generating biometric templates has completely mitigated this issue. In the same way solutions have been found and implemented to overcome many other widely publicized biometric security threats from masks, and other methods to defeat biometrics (e.g., gummy fingers).

c) Biometrics, contrary to what has been propagated in the media, are fundamentally security- and privacy-enhancing technologies. Biometric based security systems also enjoy two critical advantages over traditional computer-based security. First, biometric tokens can never be forgotten, can be as complex as the security application requires, and do not need to be written down. Second, a properly implemented biometric system offers positive attribution of who is accessing the application, where, and when.

4. **Exhibited and potential harms of a particular biometric technology**: Consider harms including but not limited to: Harms due to questions about the validity of the science used in the system to generate the biometric data or due to questions about the inference process; harms due to disparities in effectiveness of the system for different demographic groups; harms due to limiting access to equal opportunity, as a pretext for selective profiling, or as a form of harassment; harms due to the technology being built for use in a specific context and then deployed in another context or used contrary to product specifications; or harms due to a lack of privacy and the surveillance infrastructure associated with the use of the system. Information on evidence of harm (in the case of an exhibited harm) or projections, research, or relevant historical evidence (in the case of potential harms) is also welcome.

**Comments:**
a) When looking at the possible harm from biometric systems, it is critical to understand that the technology itself is incapable of doing harm. What biometric technologies can do is tell their operators things about images and signals. As has been noted here, biometric applications can be designed to recommend several classes of results. First, they can provide positive identification. Positive identification reports the identity of an individual based on an assertion of identity or a question of identity (“Who is this?”). Negative identification, on the other hand, is the question of whether a person is not in a group of interest. An example of this is the “watch list” application. In both positive and negative identification tasks, the accuracy and the performance of biometric systems can be measured and any harm can then be documented based on the performance of the system.

b) Inference applications on the other hand are not as clear or easy to measure. Inference applications attribute feeling or intentions to individuals based on biological indicators. The performance and accuracy of these inference biometrics are not anywhere near as accurate as traditional applications that verify identity.

c) Potential harm coming from the use of biometrics can take two possible forms. The first is in the performance/accuracy of the biometric system, and second for the improper use of the technology. Harm can be intentional or unintentional. There are few cases in the United States of biometrics that are designed to be intentionally harmful to the subjects of the system. Intentional harm created by a biometric system is generally easily seen and mitigated in many ways. On the other hand, unintentional harm exists in many systems all around us. Preventing unintentional harm requires an understanding of the engineering design of the application and its intended use. Unintentional harm can come from issues with the accuracy or performance of the system, the reliability of the system, or in bias in the design of a biometric system. There are generally three major categories of unintentional harm that result from poor design or incorrect use of biometric systems. The first is incorrect or inappropriate action taken by the operator of the systems as a result of an incorrect biometric match. This can take many forms based on what the specific function of the system, either government or commercial, may be. The second category of harm involves the loss of privacy. In this case, the security design of a biometric system needs to guard against the loss of privacy. The last major category involves the loss of anonymity. People expect the ability to come and go and live their daily lives without a) having to prove their identity unnecessarily and b) not have their every move, action, and interaction with others monitored, recorded, and correlated. Biometric technology offers both commercial entities and government to collect and manage this data about people.

d) When they build a system, any good engineer or designer evaluates the performance of the system and, to the extent they know the application of the system, they mitigate any potential harm that the system they design may cause.

e) In order to ensure that biometric systems are both reliable and unbiased requires extensive testing of these systems and transparency in their design and operation. Currently, there is little testing or transparency in the commercial use of biometric systems. Both commercial and government use of biometric systems need greater visibility and more testing in order to improve performance and to increase the public confidence with respect to their usefulness.
f) In order to proactively deal with potential unintentional harm from poor performance or bias in biometric systems, standards for performance, testing, and transparency must be established and good designs produced and reviewed by licensed (professional engineers, for example) professionals.

5. **Exhibited and potential benefits of a particular biometric technology**: Consider benefits including, but not limited to: Benefits arising from use in a specific domain (absolute benefit); benefits arising from using a specific modality of biometric technology (or combination thereof) compared to other modalities in a specific domain (relative benefit); and/or benefits arising from cost, consistency, and reliability improvements. Information on evidence of benefit (in the case of an exhibited benefit) or projections, research or relevant historical evidence (in the case of potential benefit) is also welcome.

**Comments:**

a) The availability of biometric data sensors continues to increase in the US and across the world. The primary biometric sensor is the digital camera. The use of internet connected digital cameras and audio devices are common, both in public places and more so in homes. Also, the reliability and accuracy of biometric systems continue to improve. With these improvements in performance, security applications of biometrics significantly benefit a wide range of users.

b) Commercial application of biometrics allows for data aggregation and personalization of services. The large amounts of data about citizens collected can provide a wide range of services, customized to the individual needs and wants of the customer.

c) With the growing availability of these new technologies, there will be a wide range of future applications. Some of the most interesting new applications will include a new class of application looking at “user state.” These applications help monitor a wide range of emotions and medical conditions.

6. **Governance programs, practices or procedures applicable to the context, scope, and data use of a specific use case:**

**Comments:**

a) Governance is critically important at this point in the life cycle of the technology. The process of governance will involve the development of policy, process, regulation, and law. However, the biggest issue in governance is trust. Unfortunately, trust is a function of many things, a good deal of which are not based on truth about the technology. Biometrics have suffered from misrepresentation in the press, movies, and other media. All governance must be based on the best possible science and engineering.

Information regarding:

- Stakeholder engagement practices for systems design, procurement, ethical deliberations, approval of use, human or civil rights frameworks, assessments, or strategies, to mitigate the potential harm or risk of biometric technologies;
Comments:

b) Stakeholder engagement is critical for any governance; however, it is critical that the governance that the US government is currently considering for the biometrics industry prioritize the interests of the people of the United States. There are a lot of vocal stakeholders whose interests are different than the interests of the public. Commercial industries’ (e.g., the major electronics and social media companies) interests are based on profitability and many undisclosed interests including the collection and control of personal data on as many people as possible. Additionally, there are a number of activists whose interests are based on specific political agendas.

c) The interests of the US public are many faceted. Their interests fall into five major categories, including: safety, security, privacy, access to services, and non-discrimination.

- Safety: Law enforcement is critical to establishing safety and rule of law. The correct use of biometrics (e.g., fingerprint, face, and DNA) is critical to physical evidence and accountability.
- Security: The security of the nation is in the interest of all citizens, and biometrics is an important tool of national security and the intelligence community.
- Privacy: Individuals have an interest in their privacy. Although biometrics are not inherently an anti-privacy technology, many applications of the technology, if not used correctly, can encroach on privacy.
- Access to services: One of the most prevalent applications of biometrics is to use identity to customize a wide range of services.
- Non-discrimination: Non-discrimination is an absolute requirement and can be achieved through careful technical planning and testing.

By doing careful design and testing the biometrics community can meet all of these objectives. These interests should be the only factors traded against each other and not political agendas or profit.

- Best practices or insights regarding the design and execution of pilots or trials to inform further policy developments;

Comments:

d) The development of best practices in the field of biometrics is already under way. In December of 2020, the Federal ID community published a community-developed document, Biometric Face Recognition: References for Policymakers (https://www.mitre.org/publications/technical-papers/biometric-face-recognition-references-for-policymakers) This document should serve as a guide to the development of biometrics policy.

- Practices regarding data collection (including disclosure and consent), review, management (including data security and sharing), storage (including timeframes for holding data), and monitoring practices;
Comments:

e) The industry has yet to create a way to perform meaningful informed consent. This is one of the most important issues that needs to be resolved as part of any governance. Because individuals do not know or understand how their data is used in the present or the future, new ways of creating consent will need to be developed. If the public doesn’t understand how their data is used then informed consent is meaningless. In addition to informed consent, data sharing and data retention must be addressed. In order to resolve these critical issues policy needs to be created to ensure that people are properly informed of the use of their data, not once but every time it is used, shared, or aggregated (e.g., grouped or linked). There are technical means to implement safeguards to data use without informing the data subjects.

- Safeguards or limitations regarding approved use (including policy and technical safeguards), and mechanisms for preventing unapproved use;

Comments:

f) Informed consent is only one of the critical aspects of biometrics safeguards. In addition, testing is critical to ensure that bias is not introduced into biometrics applications. However, if informed consent is implemented correctly, with both legal and technical safeguards, then the users will be enabled to regulate the industry themselves to a large degree. Auditing of the use of biometric data and application needs to be conducted on a regular basis by an independent agency.

g) In addition, we need to deal with the issue of data ownership. Currently, the default in the industry is that the data is owned by the organization that collects the data. In order to guarantee individual rights data needs to be owned and controlled by the individual. HIPPA has been a major consideration on protecting the rights of people with respect to their own data. However, much more needs to be done in order to preserve privacy and civil rights.

- Performance auditing and post-deployment impact assessment (including benefits relative to current benchmarks and harms);

Comments:

h) Performance auditing is critically important and must be done to validate performance of biometric systems and whether the systems are being used correctly and in an unbiased manner. In some cases, testing of biometric systems cannot be fully and effectively performed prior to the use of the systems. As the user population of the system changes the performance of systems can change and bias can be introduced. This is particularly true with AI-based systems. Post-deployment testing and validation of biometric systems need to be based on how they are used and how their user population changes. This needs to be part of the design and testing plans for the system, and any certification of the system. Testing and maintenance of the system needs to be part of any professional and responsible development plan.
• Practices regarding the use of biometric technologies in conjunction with other surveillance technologies (e.g., via record linkage);

Comments:

i) Biometrics are not a surveillance technology, though some but not all biometrics can be used for surveillance. Surveillance is by definition observing and documenting individuals’ location, movement, and actions without their consent or knowledge. Surveillance is needed in some applications and for some specific reasons. The determination of whether an application is appropriate is an evaluation of the benefits versus potential harm. The bigger and more difficult issue is not the use of biometrics data for a specific, singular application but rather the aggregation of data about individuals across time and multiple, different applications. Biometrics can make this more complex because of the increasing reliability of biometrics and their ability to ensure that data is associated with an individual identity. Data aggregation is the single greatest danger to privacy. Combatting data aggregation will require a regulatory approach specifically developed to address the issue.

• Practices or precedents for the admissibility in court of biometric information generated or augmented by AI systems;

Comments:

j) Fingerprints and DNA have been used extensively in the courts. As more biometrics are used it is important that there are standards for the technology and for the experts.

k) The use of AI-based technology in biometrics does create a number of issues for court testimony. To begin with, the experts must be very familiar with the inner working of any technology that is used and for which they testify. This can be problematic in multiple ways. First, not all AI based technology used in the industry is well understood by all biometrics experts. This is due to the fact that the companies that make these systems use trade secrets. Second, many AI systems are not transparent in their inner working because of the nature of the training algorithms they use. Finally, many biometrics experts are not also AI experts. In order to mitigate these issues, a number of steps need to be taken: 1) Biometrics experts need to be well trained and certified on all aspects of the technology that they are working with. 2) AI based biometric systems need a higher degree of transparency. 3) Some group of very experienced senior level experts need to supervise the certification of experts in this area. In addition, as with any evidence that is used in court, the testimony needs to be backed up by a body of scientific studies, formalized testing and published research. The IEEE (Institute of Electrical and Electronics Engineers) started this process several years ago with biometric professional certification program.

• Practices for public transparency regarding: Use (including notice of use), impacts, opportunities for contestation and for redress, as appropriate.
Comments:

1) Transparency is incredibly important. Transparency overlaps with a number of other issues and needs of the community, and needs to address several key factors:
   - Transparency of the design of the system, reviewed by technically competent experts.
   - Transparency of the algorithms, the ways the system makes its decisions about matching.
   - Transparency of applications, in what applications the algorithms and data are used.
   - Transparency of data use, how and when individual’s data are used.

In addition to data ownership and better-informed consent, transparency will address most of the issues with biometric and AI technologies.

Additional concerns

In order to effectively address the use of biometrics in government and industry it is critical that several major issues be addressed in the development and implementation of governance.

1. Equity and Bias: Any science can be misused or used incorrectly. Equity and bias can be designed out of any system by expert engineers.

2. The rights to anonymity / ownership of data: The right to anonymity is important to most individuals and is quickly eroding in 21st century America and throughout the world. As a part of biometrics governance, we should also more specifically specify the rights to anonymity in the United States. Likewise, the people need to be given full rights to control the use of their data and to decide how and when it will be used to target them.

3. Economic incentives: Economic incentives inherently drive behavior of commercial businesses. The data that many electronics, on-line shopping, and social media companies are collecting on people is valued in the trillions of dollars. Any regulations and governance of the biometrics industry inherently requires addressing the economic incentive to industries that collect, share, group, integrate and use this data.

4. In evaluating biometrics governance, it is necessary to create and use tools that can evaluate biometric systems in a meaningful way based on benefits and risks, and can create an ability to do trade space analysis when it comes to biometric technology selection, and test as part of an overall system and/or ensemble of other biometrics for defined applications (i.e., the trade space is not the same for different applications, but the framework/ process would be foundational). Additionally, the development of the governance will be complex and its impact should be evaluated incrementally by creating a roadmap that captures needed advances in technology, governance, regulations, and incentives for different problem domains (i.e., the governance for industry should not be the same as for national security of law enforcement). Finally, A part of this needs to include a meaningful risk analysis framework across many of the dimensions of use and reliability of the technology and benefits to the individuals.