SCIENCE & TECHNOLOGY POLICY INSTITUTE

Synopsis of Responses to OSTP's Request for Information on the Use and Governance of Biometric Technologies in the Public and Private Sectors

Thomas D. Olszewski
Lisa M. Van Pay
Javier F. Ortiz
Sarah E. Swiersz
Laurie A. Dacus

March 2022

Approved for public release distribution is unlimited

IDA Document D-33070

Log: H 22-000168

IDA SCIENCE & TECHNOLOGY POLICY INSTITUTE
1701 Pennsylvania Ave., NW, Suite 500
Washington, DC 20006-5805

The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication

This work was conducted by the IDA Science and Technology Policy Institute (STPI) under contract NSFOIA-0408601, project TP-20-1005.DH, "Assessing Use and Governance of Biometric Technologies in the Public and Private Sectors," for the Office of Science and Technology Policy. The views, opinions, and findings should not be construed as representing the official positions of the National Science Foundation or the sponsoring agency.

For More Information

Thomas D. Olszewski, Project Leader
tolszews@ida.org, 202-419-5476

Kristen M. Kulinowski, Director, Science and Technology Policy Institute
kkulinow@ida.org, 202-419-5491

Copyright Notice

SCIENCE & TECHNOLOGY POLICY INSTITUTE

IDA Document D-33070

Synopsis of Responses to OSTP's Request for Information on the Use and Governance of Biometric Technologies in the Public and Private Sectors

Thomas D. Olszewski
Lisa M. Van Pay
Javier F. Ortiz
Sarah E. Swiersz
Laurie A. Dacus

Executive Summary

On October 8, 2021, the Office of Science and Technology Policy (OSTP) posted a Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies (the "Biometric RFI").[1] The purpose of the RFI was "to understand the extent and variety of biometric technologies in past, current, or planned use; the domains in which these technologies are being used; the entities making use of them; current principles, practices, or policies governing their use; and the stakeholders that are, or may be, impacted by their use or regulation." In conjunction with the RFI, OSTP also hosted two public listening sessions (November 18 and 29, 2021) for individuals to share oral comments. This report provides the Science and Technology Policy Institute's synopsis of both oral comments expressed in the listening sessions and written responses submitted to the RFI.

A total of 225 participants attended one or both listening sessions and 53 individuals made 74 separate comments (some participants spoke more than once). Although industry representatives were the most numerous attendees (71 total), representatives of civil society and advocacy organizations were the most numerous speakers (28 speakers). Listening session participants provided a variety of perspectives on their perceptions of biometric technology, various societal concerns, and numerous policy recommendations.

A total of 130 written submissions were received in response to the Biometric RFI, totaling more than 1,000 pages. Forty-seven submissions (36%) represented perspectives from industry, 38 (29%) from non-profit foundations and advocacy groups, and 26 (20%) from academia (the rest [15%] came from unaffiliated respondents, government, and labor unions). Respondents described a wide variety of uses of biometric technologies, some providing benefits and others resulting in harms to individuals or society. Numerous submissions addressed the validation, use, and limitations of biometric technologies driven by artificial intelligence. Although opinions ranged widely on how, when, and where biometric technologies should be implemented and their potential consequences for individuals and society, several general concerns emerged as common themes:

- privacy and the ability of individuals to control access to and use of their biometric data;

[1] Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies, 86 Federal Register 56,300 (October 8, 2021). https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies

- discriminatory bias in AI-powered biometric systems;
- chilling freedom of speech and association due to biometric surveillance;
- the security of sensitive biometric information; and
- defining clear boundaries on where, when, and how biometric technologies can be used.

In addition to examples, almost all submissions included recommendations on how to govern and manage the use and future development of biometric technology and data. Although opinions ranged widely, a number of fundamental policy principles were consistently voiced by numerous respondents from all perspectives:

- Give people ownership and agency over their own data as a fundamental right.
- Avoid bias and discrimination.
- Build on existing law and regulations governing non-discrimination, privacy, civil liberties, and human rights.
- Be evidence-based.
- Apply guidelines and regulations to well-defined use cases rather than focusing on specific technologies.
- Balance benefits and risks and particularly consider the elevated risks of vulnerable populations.
- Establish guardrails that promote innovation and prevent harmful use cases.

Contents

1. Introduction and Background

On October 8, 2021, the Office of Science and Technology Policy (OSTP) posted a Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies (the "Biometric RFI").[2] The purpose of the RFI was "to understand the extent and variety of biometric technologies in past, current, or planned use; the domains in which these technologies are being used; the entities making use of them; current principles, practices, or policies governing their use; and the stakeholders that are, or may be, impacted by their use or regulation."[3] The RFI requested responses by January 15, 2022, and comments received by the first subsequent business day—January 18, 2022—are incorporated into this synopsis. In conjunction with the RFI, OSTP also hosted two public listening sessions (November 18 and 29, 2021) for individuals to submit oral comments.

OSTP asked the Science and Technology Policy Institute (STPI) to facilitate the listening sessions and to prepare a written report summarizing both oral comments expressed in the listening sessions and written responses submitted to the RFI.

For the purposes of the RFI, "biometric information" refers to "any measurements or derived data of an individual's physical (e.g., DNA, fingerprints, face or retina scans) and behavioral (e.g., gestures, gait, voice) characteristics."[4] Although any comments addressing the use of biometric technologies in the public and private sectors were solicited, OSTP identified six particular topics of interest:[5]

1. Descriptions of use of biometric information for recognition and inference;
2. Procedures for and results of data-driven and scientific validation of biometric technologies;
3. Security considerations associated with a particular biometric technology;
4. Exhibited and potential harms of a particular biometric technology;
5. Exhibited and potential benefits of a particular biometric technology; and

---

2 Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies, 86 Federal Register 56,300 (October 8, 2021). https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies

3 Ibid.

4 Ibid.

5 Ibid.

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

This synopsis is based on 74 oral comments made during the listening sessions and over 1,000 pages of written comments submitted to the RFI. The oral and written comments were treated separately due to the different level of detail that each mode could accommodate. In addition, a number of listening session speakers also submitted written comments; their oral and written contributions were treated separately and incorporated into the corresponding sections of this document. Thirty listening session attendees (13 of whom spoke) also submitted written comments.

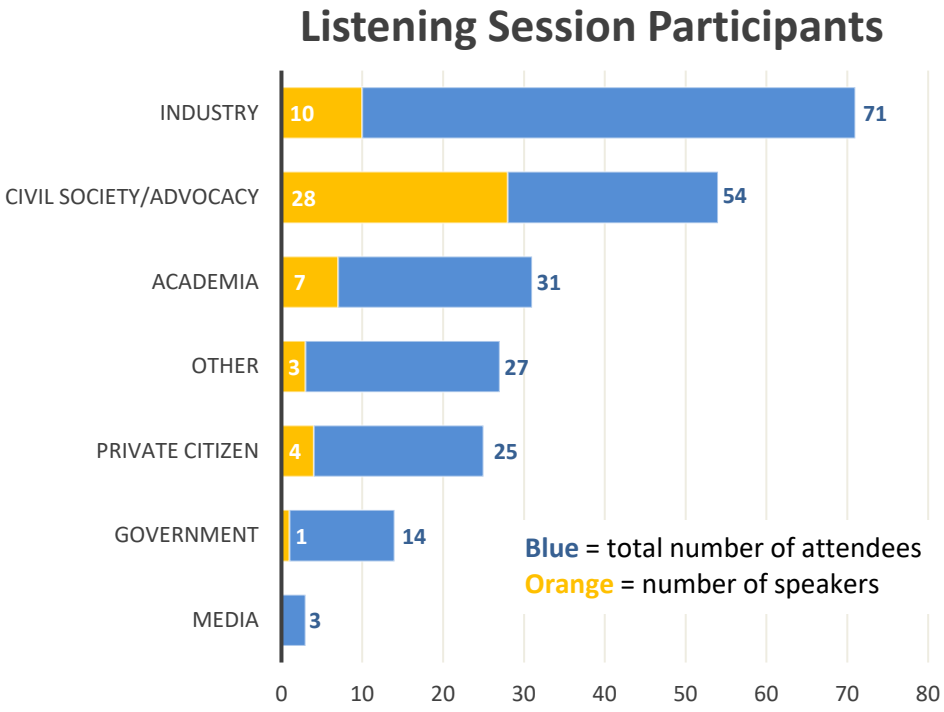
The purpose of this report is to identify recurrent and common themes in the RFI submissions and provide the reader with an overview organizing the many disparate comments, opinions, and recommendations provided by RFI respondents. Although this report aims to provide as thorough a summary of the oral and written comments received by the RFI as possible, its brevity allows it to capture only the general sense of respondents' submissions. It is not a replacement for the original comments submitted by respondents expressing their thoughts and concerns regarding biometric technology in their own words, which have been publicly posted by OSTP.[6]

All statements and opinions reported in this document are based on submitted comments. **All RFI respondents' statements were accepted at face value; no attempt was made to verify or fact-check claims made in oral or written submissions.** Numerous sometimes contradictory statements and opposing opinions were received; to avoid the perception of favoring particular submitters, these are not directly cited in this document. Inclusion of comments or recommendations derived from Biometric RFI submissions in this report does not represent endorsement by STPI or OSTP.

[6] Public Input on Public and Private Sector Uses of Biometric Technologies: https://www.ai.gov/86-fr-56300-responses/

2. Public Listening Sessions

In support of OSTP's RFI on Public and Private Sector Uses of Biometric Technologies, STPI facilitated two OSTP-hosted virtual public listening sessions on Thursday, November 18, 2021 from 4:00–6:00 p.m. eastern time and Monday, November 29, 2021 from 7:00–9:00 p.m. eastern time. The format allowed speakers to address any aspect of the use and governance of biometric technologies in turns of 2 minutes. Between the two events, 225 participants representing a variety of societal sectors (Figure 1) attended for at least part of one or both sessions, and 53 individuals spoke or contributed comments (one person spoke at both sessions and several people delivered more than one comment). Speakers addressed a wide range of technological issues, societal concerns, and policy considerations.



Note: Categories were self-identified by participants at the time of registration ("Other" included entities like law firms, scientific societies, and research organizations). Although industry was represented by the largest number of attendees, almost half of all speakers identified themselves as representing civil society or other advocacy organizations.

Figure 1. Number of Individuals Who Attended and Spoke at One or Both Biometric Listening Sessions

The listening sessions were summarized by identifying recurrent themes based on detailed notes taken by STPI staff and supplemented with automated transcripts generated by the virtual meeting software (Zoom for Government). Comments from the two listening sessions were combined into one summary to avoid repeating similar themes and topics raised at both.

A. Perceptions of Biometric Technology

Through the course of both listening sessions, participants discussed numerous types of biometric information—voice/speech, text/typing, biomedical information, fingerprints, eye/iris, gait/movement—but the single most frequently mentioned technology was facial recognition. Listening session speakers noted that biometric technologies (and particularly facial recognition) are used for non-identifying detection of human presence (for example, pedestrian warning systems in cars), to verify an individual's identity (one-to-one comparison like that used to unlock smart phones), to identify unknown individuals (one-to-many comparison of a captured image to a database of known individuals using artificial intelligence [AI]), and to evaluate an individual's emotional state based on biometric information.

A frequently expressed concern was the widespread deployment of immature and unvalidated biometric technologies with unknown risks of causing harm. Listening session speakers noted the frequent failure of biometric identification via facial recognition under non-ideal conditions (for example, one speaker described how ride-share drivers who must log into service networks can be locked out of work or payment in poor or dim light). Multiple speakers noted that biometric systems designed for the evaluation of emotional or mental state based on facial expressions, voice patterns, or typing can misclassify people with disabilities or with foreign accents. Lastly, speakers noted that AI algorithms used for biometric analysis can be opaque and their accuracy can be compromised when trained on data not representative of the population to be analyzed. There was widespread acknowledgment by listening session participants of the need to strongly validate biometric technologies to ensure they are acceptably accurate and fair.

B. Societal Concerns Raised

Speakers in the listening sessions voiced a wide range of concerns about negative societal and social impacts resulting from the use or misuse of biometric technologies, many of which stemmed from documented or potential discriminatory outcomes based on race, gender, gender orientation, disability, and language or accent.

A repeatedly voiced concern centered on misuse of biometric technology by government to carry out non-consensual mass surveillance. Several speakers reported that the use of facial recognition to monitor crowds and protests could lead to the chilling of legitimate first amendment activities. Other speakers suggested that use of biometric

technologies to monitor inmates in prisons could result in violation of civil rights. Several participants cited examples of wrongful arrest, particularly in the case of people of color, resulting from incorrect results of facial recognition technology. Similar errors arising from incorrect biometric results that have led to the denial of unemployment benefits were also reported during both listening sessions.

Several concerns over the potential for misuse of biometric technologies in the education sector were raised during the listening sessions. First, many speakers argued that non-consensual surveillance violates students' civil rights and undermines the need for educational environments to be conducive to learning and development rather than being punitive and carceral. Second, with the shift to widespread remote learning in the wake of the COVID-19 pandemic, biometric technology has been used to determine online attendance; however, speakers noted that errors in biometric identification can penalize students unfairly, particularly people of color, due to discriminatory biases in identification algorithms. Lastly, several listening session participants expressed concern that the use of biometric data to monitor or predict behavior tends to unjustly criminalize racial minorities, again due to discriminatory bias built into the AI algorithms used.

As in the government and education sectors, participants expressed concerns about the misuse of biometric technologies in the private sector that included surveillance and mischaracterization of individuals based on biometric data. One speaker's example presented concerned the analysis of facial expressions, typing, and voice during employment interviews, which the speaker reported can produce misleading evaluations of prospective hires and particularly disadvantages people who fall outside the range of data used to train biometric algorithms (e.g., based on race, disability, gender, gender identity). In addition to surveillance and discriminatory bias, several speakers raised the issues of privacy and data ownership in relation to the private sector. A commonly expressed concern in the course of the listening sessions was the prospect of private companies selling biometric data or products derived from biometric data collected without the consent or awareness of individuals or the ability to opt-out of being included. In addition, speakers expressed concern over the security of data, particularly of potentially sensitive biomedical information, in both the public and private spheres.

C. Policy Recommendations and Considerations Voiced

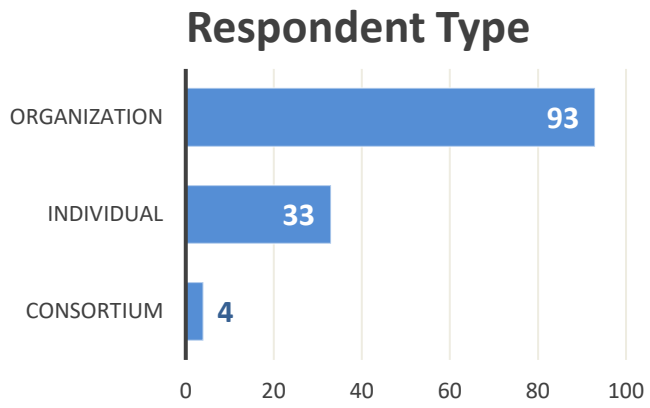
Many session speakers advocated for specific legislation or actions, with some calling for an outright ban or a moratorium until biometric technologies are more mature. Beyond specific recommendations, listening session participants suggested a number of broader principles that the Federal Government should consider as it formulates policy governing biometric technologies. First, several speakers—particularly those from the private sector or representing trade groups where biometric technologies are used—advocated for policies to be based on evidence and not to be influenced by the strong emotional responses

that biometric technology can generate. In addition, several speakers noted the need for different rules governing different types of biometric technologies and for different applications; speakers suggested that it would be better to regulate the use of a biometric technology rather than the technology itself in some cases. The importance of balancing the potential benefits of biometric technology with equity and justice for individuals was raised by virtually all speakers who addressed the issue, despite a variety of opinions on the right balance. Lastly, speakers advocated for enforcement mechanisms to ensure that entities developing and using biometric technologies can be held accountable.

3. Written Submissions

A total of 130 written submissions were received in response to the Biometric RFI from a wide variety of respondents on a diverse array of subjects related to biometric technologies and their role in civil society and economic development. Based on information contained in the submissions, STPI classified submissions by respondent type and representative sector.

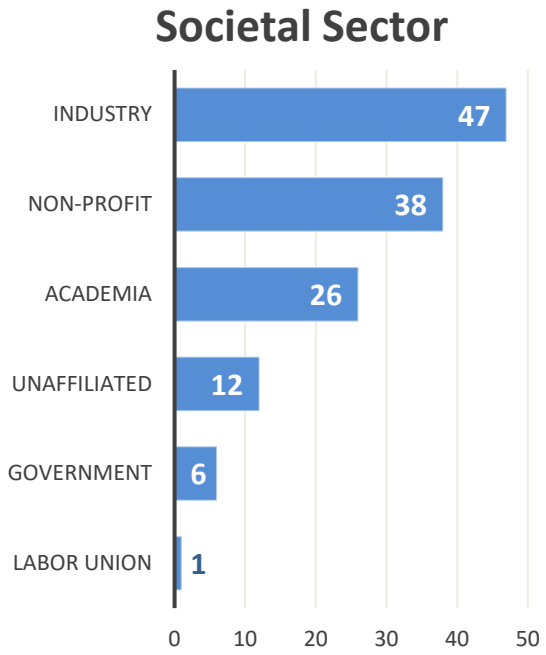
Three times as many responses were received from organizations (non-profits, advocacy groups, for-profit companies, universities, trade associations, and other comparable entities) than from individuals (including informal groups of individuals) representing their own views (Figure 2).



Note: Organizations represent any formally organized entity (e.g., for-profit companies, advocacy organizations, trade associations), individuals include single individuals and informally organized small groups of individuals, and consortia count single responses jointly submitted by multiple organizations and/or individuals.

Figure 2. Number of Entries Submitted by Different Types of Respondents to the Biometric RFI

The largest number of RFI responses, whether submitted by individuals or organizations, came from industry, followed by non-profit organizations and academia (Figure 3).



Note: Sectors were inferred from the content of submissions and represent both submissions from organizations as well as the perspectives of individuals active in various sectors. "Government" includes Federal, State, and local agencies and organizations.

Figure 3. Number of Submissions Received from Different Societal Sectors to the Biometric RFI

Synopsis of the written submissions was organized around the six major topic areas identified by OSTP:

1. Descriptions of use of biometric information for recognition and inference;
2. Procedures for and results of data-driven and scientific validation of biometric technologies;
3. Security considerations associated with a particular biometric technology;
4. Exhibited and potential harms of a particular biometric technology;
5. Exhibited and potential benefits of a particular biometric technology; and
6. Governance programs, practices, or procedures applicable to the context, scope, and data use of a specific use case.

In each submission, text relevant to each particular topic area was extracted. Topic areas were not treated as mutually exclusive and a body of text could be deemed relevant to more than one. After text from all the submissions had been extracted and sorted, a summary of comments in each topic area was prepared by identifying recurrent themes.

4. Descriptions of Use of Biometric Information for Recognition and Inference

Submissions to the Biometric RFI highlighted numerous uses of biometric information for recognition and inference, providing both sector-specific and cross-sector examples. The use of biometric information is rapidly evolving, and many respondents identified shifts in attitudes toward the technology. In particular, they cited the proliferation of smartphones collecting fingerprint and facial recognition information to unlock personal devices and widespread adoption of biometric tools for COVID-19-related health protocols as drivers of adoption.

A. Public Sector Uses

RFI respondents identified uses of biometric information in public spaces from city streets to airports. Many noted that the collection and use of biometric information in the public sector is increasingly dependent upon private sector biometric-enabled technologies, such as facial recognition and iris scanners in airports and travel hubs. Many respondents also cited the use biometric technologies for surveillance particularly of Black communities by law enforcement agencies across all levels of offenses, including non-violent crimes and misdemeanors.

The adoption of technologies that incorporate an array of physical and behavioral biometrics by public schools and universities was raised in multiple RFI submissions. Uses in educational settings listed by respondents included support for remote-learning software and remote-proctoring tools, collection of behavioral information to assess students' emotional and psychological states, and experimentation with wearable biometrics, such as helmets, headsets, bands, and uniforms that provide information on students' attention and concentration levels.

Multiple RFI respondents also identified use of biometrics in systems for accessing public resources and benefits. For instance, several submitters cited the particular example of biometrics in unemployment systems. One respondent noted the Department of Veterans Affairs' use of biometric technology in virtual chronic care management.

B. Private Sector Uses

RFI respondents noted a variety of uses of biometric information in the private sector, including by vendors for consumer protection and by employers for employee monitoring. Multiple respondents noted U.S. retailers are increasingly adopting facial recognition

technology for security, and theft prevention as well as contactless payment that makes use of fingerprints and facial recognition.

Some RFI respondents addressed the use of biometric technology in specific industries. For example, one submission noted that the automotive industry is developing technologies for consumer safety and convenience, such as face detection or heartbeat sensors to ascertain whether a child has been inadvertently left unattended in the backseat of a vehicle, provide more accurate seatbelt reminders, or detect pedestrians. Another example submitted to the RFI was the use of biometric technologies in the healthcare industry for a wide variety of purposes from clinical treatment to identity verification to prevent insurance fraud. Respondents noted biometric technologies used to detect emergencies, identify patient needs, and even provide clinical decision support or treatment recommendations in healthcare settings. Respondents also communicated that health insurance providers use voice biomarkers to authenticate users and minimize opportunities for fraud. In addition to established industries, biometric information collected and used in emerging industries was mentioned in RFI submissions: for example, augmented reality and virtual reality systems collect extensive biometric data to create immersive experiences.

Several respondents noted that employers are implementing biometric systems to monitor, track, and nudge employees for safety and to increase efficiency. One submission described how some manufacturing firms in China are outfitting workers with caps that monitor brainwaves; they then adjust the frequency and length of breaks to reduce the mental stress of workers. Also in China, respondents reported the use of smart bands embedded in the uniforms of sanitation workers to track breaks and increase efficiency as well as cushions and smart bands deployed with the intention of biometrically tracking employees' physical and emotional states.

C. Notable Use Examples

Multiple RFI respondents cited DNA, fingerprints, dental records, and facial recognition as impactful biometric tools in fighting child sex trafficking and exploitation. Other respondents described the use of biometric information in humanitarian aid work, where it is used to identify and "deduplicate" aid recipients without the need for physical forms of identification that may be forgotten, lost, or stolen.

5. Procedures for and Results of Data-Driven and Scientific Validation of Biometric Technologies

Validation of the performance of biometric systems was widely acknowledged by Biometric RFI respondents as a necessity for their ethical use, particularly in addressing three interrelated concerns: poor accuracy, unwanted biases, and systemic unfairness. Another widely shared understanding among RFI respondents is that validation of biometric technologies requires more than just testing algorithms—it requires evaluating the people, processes, and technology that make up the entirety of a biometric system in the context of the risks and benefits of its intended use.

A. Data for AI-Powered Biometric Systems

RFI respondents emphasized that data used to train and test AI facial recognition algorithms should be collected transparently and with the explicit consent of individuals. In addition, it was generally agreed by submitters that algorithm training should be based on demographically representative, balanced data; one respondent noted that existing, widely used data sets that are known to be biased will need to be discarded. Several respondents pointed out that databases used for biomedical research tend to be small (for example, just tens or hundreds of individuals speaking for a few minutes in speech databases), demographically biased, and non-inclusive of people with disabilities, resulting in biometric applications that perform poorly in real-world clinical settings.

B. Evaluation of Biometric Systems

Three broad stages of biometric system evaluation were described by several RFI submitters:

1. *Technology evaluation* assesses the consistency and reproducibility of individual components and algorithms of a biometric system;
2. *Scenario evaluation* simulates a full biometric application in a controlled setting or specific use case prior to operational deployment; and
3. *Operational evaluation* examines the performance of a biometric system in the real world.

Technology and scenario evaluation were both regarded as important by respondents, but RFI respondents consistently noted that such evaluations only test a biometric system's

accuracy under controlled conditions that may not be representative of possible real-world scenarios. Several submissions also noted that operational evaluation often focuses on cost, workflow, and user experience rather than accuracy or bias and can suffer from lack of experimental control and baseline information.

A widespread theme among RFI submissions was that standardized testing is a critical tool for building successful biometric systems. Respondents argued for the importance of rigorous, independent review prior to the deployment of a biometric system and regularly scheduled monitoring of accuracy and impact throughout its operational lifecycle. In addition, several submitters encouraged disaggregating error rates by sex, race, and other context-dependent demographic characteristics to identify and correct bias. Lastly, to ensure reproducibility of evaluation results, some RFI respondents expressed support for test data sets to be publicly available or obtainable through data sharing agreements.

C. Accuracy of Biometric Systems

Numerous RFI respondents cited reports evaluating facial recognition systems published by the National Institute of Standards and Technology (NIST). Many submitters noted that the best facial recognition algorithms tested by NIST are highly accurate (accuracy rates as high as 99.97 percent) and show negligible differences in their rates of false-positive and false-negative readings across demographic groups. However, other RFI respondents noted—based on the same NIST reports—that the quality of facial recognition systems can vary significantly, with the poorest algorithms 100 times more likely to perform worse on Black, Asian, and Native American faces, as well as on women, the elderly, and children. The same submitters noted that when evaluating nationality, faces from West Africa, the Caribbean, East Africa, and East Asia resulted in more uncertainty and more false matches than those of White men.

RFI respondents emphasized that biometric systems must be evaluated under a variety of conditions—for example, facial recognition systems should be tested with varying pose, illumination, and expression—and include a representative range of people spanning gender, race, and disability.

The accuracy of biometric systems was also reported in RFI submissions to vary by type of application. In particular, respondents noted that facial recognition used for identity verification (one-to-one comparison of an individual with a known biometric profile to confirm their identity) yielded much lower error rates than identification (one-to-many comparison attempting to match an unknown individual with images in a database). Use of biometric technologies to evaluate emotions or characterize behavior based on analysis of facial expressions, gait, keystrokes, or vocal characteristics was consistently reported by RFI respondents to lack a reliable scientific foundation and to suffer from substantial inaccuracy and discriminatory bias.

RFI respondents also noted that required accuracy levels should match the intended purpose of a system—for example, a system that identifies potential bad actors should have different confidence thresholds for a match than a system intended to verify the identity of a recipient of government benefits. In addition, to acknowledge uncertainty, several submitters suggested that biometric systems should return a well-specified "confidence score" of all identification matches including "abstention" or "no result" when results are indeterminate.

D. Transparency and the Role of Humans in Biometric Systems

A common theme in many RFI submissions was the importance of transparency in the operation, deployment, and evaluation of AI-powered biometric systems: understanding how algorithms arrive at a decision promotes public trust in the responsible development and use of such technologies. Respondents also noted that opaque or "black box" AI tends to lead to less accurate decision making because such systems are harder to troubleshoot.

Many RFI submitters advocated that facial recognition systems and processes should augment rather than replace the decision-making capability of human analysts and that decisions that can affect an individual's welfare should not be left exclusively to biometric software. Many respondents also felt that biometric systems should have an embedded capacity for manual correction and improvement.

Although the importance of keeping humans in the loop was a consistent theme in RFI comments, submitters also acknowledged that human judgment carries its own biases and that operators can influence the outcome of a biometric analysis through the decisions they make, like setting thresholds for identification or choosing particular images for comparison. Many RFI respondents also pointed out that advances in machine learning present an opportunity to reveal human biases and to be deliberate and transparent in mitigating them.

6. Security Considerations Associated with Particular Biometric Technologies

Comments submitted to the Biometric RFI touching on security largely fell into two broad, interrelated categories: keeping biometric data secure (cybersecurity) and concerns about the consequences of biometric data breaches (individual privacy). Many RFI respondents expressed concern that personally identifiable biometric information that is increasingly commonly collected for use in a variety of sectors—including healthcare, employment, law enforcement, education, finance, and government services—could be hacked, stolen, sold, or misused. On the other hand, other RFI respondents described how biometric information can strengthen the security of digital information, both biometric and otherwise.

A. Cybersecurity of Biometric Information

Although biometric data are not a cybersecurity panacea, many RFI submitters noted that they can be an instrumental part of a multi-factor authentication system integrating biometric technologies with more traditional methods (e.g., passwords, verification codes). The power of biometric technologies for identity verification—i.e., determining whether someone is who they claim to be by comparing their biometric information (face, fingerprint, voice, iris) with a saved biometric profile—was noted in numerous RFI submissions. Respondents mentioned two ways to ensure that the profiles used for authentication are themselves not fake: operators of biometric databases can require in-person enrollment or individuals could permit government agencies that issue credentials (e.g., the Social Security Administration at the Federal level or motor vehicle driver licensing agencies at the State level) to validate information.

A number of RFI respondents addressed concerns over attempts to spoof biometric data through identity-based methods like using a voice recording or a deepfake video (a synthetic video in which a person in an existing video is replaced with someone else's likeness). Although currently available technology is effective at thwarting impostor attacks (attacks using an image or other biometric data of a different person pretending to be the asserted identity) and presentation attacks (attacks using masks or recordings of the asserted identity to gain access), one submitter particularly noted that digital injection attacks, which bypass sensors (e.g., camera, microphone, fingerprint reader) and feed synthetic information directly into an identification data stream, remain difficult to detect at this time. However, as noted by multiple respondents, cybersecurity is an arms race

between malicious actors and data stewards and it is always necessary to adapt to new and innovative forms of attack.

A few RFI respondents expressed concern that biometric data may leave people particularly vulnerable to identity theft because biometric information is derived from fixed traits of an individual. However, a larger number of respondents pointed out that raw biometric data (e.g., images of faces and fingerprints, recordings of voices) are typically converted into formats from which neither the original information nor the biometric attributes can be reconstituted. In addition, RFI comments from technology developers noted that stored, formatted data can be further encrypted using biometrically enabled techniques, providing an additional layer of defense.

B. Privacy and Individual Security

In addition to the use of biometric technologies as a means of strengthening cybersecurity, many RFI respondents raised concerns about potential violations of individual privacy stemming from security breaches of personal biometric information. RFI respondents widely recognized that biometric data share many of the same cybersecurity vulnerabilities to insider threats and external hacks as any other form of digital data and advocated the following best practices:

- biometric data should be strongly encrypted when stored and transmitted;
- all activity accessing or modifying biometric data should be logged and fully auditable;
- access to biometric data should be limited to authorized users with a clear need; and
- biometric data should not be retained longer than needed for their intended purpose.

A consistent and common theme expressed by RFI respondents from all sectors, from civil society advocates to commercial providers of AI-powered biometric technologies, was the importance of informed consent for the collection, use, and sharing of biometric data. In addition to consent, numerous RFI comments argued for the importance of alerting individuals should their biometric data be affected by a data breach, providing means of redress should biometric data be used or shared inappropriately, and removing or correcting erroneous or inaccurate biometric information. The issue of privacy is additionally complicated in the case of genetic data, which a few respondents noted is not only immutable and uniquely identifiable for individuals during their lifespan and after death, but can also be linked to relatives and offspring via common heredity.

A concern frequently expressed in Biometric RFI submissions was the invasion of individual privacy stemming from non-consensual use of facial recognition technology for open-ended surveillance.

Concerns and constraints surrounding privacy of biometric information were raised by RFI respondents in a number of specific sectors:

- In the arena of government, several submissions mentioned the Privacy Act of 1974,[7] also known as the "Code of Fair Information Practices," which requires Federal agencies to "balance the government's need to maintain information about individuals with the right of individuals to be protected against unwarranted invasion of their privacy and to limit the unnecessary collection of information about individuals."
- In the education sector, multiple RFI respondents acknowledged that although there is good reason to hold onto students' records for the duration of their academic career, several felt that any biometric information gathered from virtual attendance or on-site surveillance should be retained for only the shortest possible time. In addition, the requirement to obtain parental consent before a student's biometric records can be released, enshrined in the Family Educational Rights and Privacy Act,[8] was recognized in at least one Biometric RFI submission.
- In the health sector, RFI respondents expressed concern that AI-driven biometric technology is capable of and could be used to analyze materials like emails or social media posts to access personal health information about users without their consent or knowledge. In this case, submitters noted that the Health Insurance Portability and Accountability Act[9] applies safeguards for patients' sensitive health information and requires covered entities to notify individuals in the event of a breach of personal health information, including biometric identifiers.
- In the area of law enforcement, RFI respondents noted that police use of facial recognition for image matching and identification remains entirely unregulated in most States and at the Federal level. Of particular concern was the relationship between U.S. Immigration and Customs Enforcement and private sector biometrics contractors, about whose use, collection, and third-party

---

7 Privacy Act of 1974, 5 U.S.C. § 552a (1974): https://www.law.cornell.edu/uscode/text/5/552a

8 Federal Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g: https://www.law.cornell.edu/uscode/text/20/1232g

9 Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. § 1320d: https://www.law.cornell.edu/uscode/text/42/1320d

sharing (including with foreign governments) of data little is publicly known and who RFI respondents report have received exemptions from Privacy Act requirements.

7. Exhibited and Potential Harms of a Particular Biometric Technology

A. Algorithmic Bias

Numerous RFI respondents highlighted or expressed concerns for the exhibited and potential harms of biometric technologies at large, as well as for specific designs and use cases. Biometric technologies rely on extensive source data in order for algorithms to develop experience identifying patterns and making decisions based on those patterns; however, submitters to the Biometric RFI noted that limitations in the training datasets (image quality and sourcing, extensivity, representation of different demographic groups) and human-developed AI models can lead biometric algorithms to perpetuate discriminatory biases and harms. Across the spectrum of biometric technologies, but especially facial recognition technologies, respondents provided detailed information regarding the inconsistent performance of biometric algorithms for distinct application areas and demographic groups (including gender, race/skin color, age, and disability).

1. Gender Bias

RFI respondents identified consistent inaccuracies and biases in facial recognition technologies for gender identification. One RFI submitter cited a 2018 study ("Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification") on gender classification algorithms that found three commercial systems achieved greater accuracy on male faces compared to female faces, while performing worst on darker-skinned female faces.

Many Biometric RFI respondents noted that misidentifying and misgendering faces can cause serious harm. For example, one submission outlined how facial recognition is increasingly being integrated with clinical decision support systems to analyze patient biomedical data and provide treatment suggestions, but when women and trans people are underrepresented in training datasets, the AI algorithms can fail to account for special medical needs, resulting in decreased quality of patient care.

2. Race and Skin Color Bias

Many RFI respondents noted that systemic errors and failures arise when identifying non-White individuals. With facial recognition, respondents reported studies that revealed that Black and East Asian individuals are between 10 to 100 times more likely to be falsely identified compared to Caucasian faces, while false negative rates are highest for East

Asian and Native American faces. RFI respondents also noted that voice recognition systems exhibit notable unreliability for certain accents.

Numerous respondents described how racial algorithmic biases contribute to real harm. In the law enforcement sector, many submissions described incidents of wrongful arrest and detainment due to false biometric identification. Furthermore, submissions widely acknowledged that the historical overrepresentation of Black people in arrest records and police databases, such as the Next Generation Identification system of biometric data, further contributes to inaccurate, racially-biased algorithmic predictions for criminal activity and recidivism.

3. Age Bias

RFI respondents also noted that biometric technologies have displayed failures to identify individuals by age, both young and old. Submitters specifically noted 1) facial recognition algorithms exhibiting greater misidentification rates for children, 2) fingerprint technologies misreading prints for youth (whose fingerprints do not stabilize until adolescence), 3) difficulty using flat plate fingerprinting systems for people with arthritis, and 4) diminished accuracy in iris scans of individuals with cataracts. The application of facial recognition systems in educational settings sparked concern from numerous RFI respondents, who argued that the use of systems that are inaccurate for children can lead to wrongful disciplinary action, especially for children of color.

4. Disability Bias

Multiple submissions pointed to the data and design failures for differences in facial expression, speech patterns, gestures, eye movement, and mobility that lead to misidentification, misuse, and resulting negative impacts on disabled populations. In the educational sector, respondents noted that this can lead to the misidentification of cheating on exams, where facial recognition systems fail to account for students with disabilities. In addition, several submitters expressed concern that companies using virtual hiring programs enabled by biometric systems may not be aware of the shortcomings of the technology; instead, hiring managers may take the algorithmic inferences at face value, including those that assign lower cognitive scores, job aptitude scores, and negative emotions to disabled candidates.

B. Privacy and Security

In addition to the widespread concerns among RFI submitters regarding unrepresentative data, inaccurate analyses, and biased decision making by biometric systems, another major category of harms identified by respondents revolves around issues of privacy and security. Under this umbrella are concerns with 1) data use and security, and 2) surveillance and privacy issues.

1. Data Use and Security Harms

Concerns reported by RFI respondents focus on the use and collection of potentially sensitive biometric data by institutions and corporations. With biometric technologies spanning many modalities (from facial images to DNA) and potential areas of application, many RFI respondents raised questions and concerns about data protection principles such as data minimization, purpose transparency, and general accountability. RFI submissions reflected a wider dispute about who should have visibility, control, and ownership of data captured by biometric systems. Biometric data collected without consent for AI model training, protected storage of personally sensitive data, or future sale to third parties were all concerns expressed widely in RFI submissions. As a specific example of the sensitive nature of biometric data noted in one submission, DNA can provide information on an individual's ancestry and phenotypic traits.

2. Surveillance and Privacy Harms

Another persistent theme in RFI submissions revolved around the use of biometric systems for indiscriminate surveillance and its potential normalization. Many submissions noted that such surveillance violates constitutional protections as well as existing laws covering protected populations such as children. For personally identifiable information, respondents noted that the Privacy Act of 1974[10] limits the collection of this information by Federal agencies to cases where it is "legally authorized and necessary" and mandates protection of these data to prevent intrusions on privacy. However, in applications such as the use of biometric technologies in schools, several RFI respondents expressed concern that children may be desensitized to constant surveillance and monitoring by these systems, despite their young age and questions regarding their ability to consent.

[10] Privacy Act of 1974, 5 U.S.C. § 552a (1974): https://www.law.cornell.edu/uscode/text/5/552a

8. Exhibited and Potential Benefits of a Particular Biometric Technology

A. Law Enforcement

Since the earliest use of fingerprints, the variety of biometric modalities used in law enforcement has expanded to include face, iris, voice, and DNA. RFI respondents acknowledged that facial recognition technology, along with other biometric technologies such as fingerprint detection and DNA (via family submissions to the Federal Bureau of Investigation's CODIS DNA database), has been employed as a tool to help recover victims of human trafficking and to identify unknown human remains. RFI submitters also acknowledged the usefulness of biometric tools combatting terrorism, notably the use of facial recognition to identify suspects who made terrorist threats and potentially avert future attacks. Lastly, biometric technologies were mentioned in numerous RFI submissions as tools used for the identification of individuals responsible for various crimes ranging from shoplifting to armed robbery to murder, although respondents generally stressed the importance of human involvement and oversight when using biometric tools to identify criminal suspects.

B. Airport Security and Experience

Airports and other customs/border crossings were also mentioned in RFI submissions as settings where biometric systems have been implemented to increase passenger safety, improve traveler experience, and more recently, reduce risks of COVID-19 exposure. Facial recognition was mentioned by some submitters to be an effective enabler for rapid and efficient identification across multiple points within an airport, from border checkpoints to passenger check-in. In the United States, the voluntary Global Entry program uses facial recognition and fingerprint data to provide expedited screening for travelers returning from outside the country, which some RFI respondents noted has partially automated the time-intensive task of identity verification, thereby allowing security personnel to focus their time and expertise on higher risk cases.

C. Financial Services and Transactions

The implementation of biometric technologies for identity verification, from traditional banks to e-banking mobile applications, was mentioned in RFI submissions from the financial sector. Systems that apply both facial recognition and advanced algorithms can help prove the identity of customers seeking banking services or loans,

which RFI respondents noted is especially useful for populations with limited credit report data or without multiple forms of government identification, such as younger people, immigrants, and historically marginalized groups. For phone-call banking services, RFI respondents noted that voice verification technology has provided a reliable identity check for many years, enabling customers to make account inquiries. In addition, the importance of facial recognition and fingerprint detection in confirming individual identity and preventing attempts at fraud and unauthorized logins with the rise of digital banking apps that offer handheld access to account information and transactions was noted in numerous RFI submissions.

D. Healthcare

In contrast to the prevailing use cases in sectors such as law enforcement and financial services, RFI submitters focused less on the use of biometric technologies for rapid identification within the healthcare sector. Instead, respondents more frequently addressed systems that combine biometric modalities with advanced algorithms as a tool in the provision of healthcare. In particular, respondents mentioned the use of biometric technologies to help improve patient experience, remotely monitor patients, and optimize diagnoses. For example, several submissions described wearable devices that capture and store biometric information including vital signs, activity levels, and sleep patterns; these devices provide valuable insight into patient health and offer the opportunity for medical professionals to prescribe a more personally tailored treatment plan. In addition, such devices collect and transmit information remotely, which RFI respondents noted enable new insights and treatments without an in-person appointment. Voice recognition technologies have also been used in healthcare—for example, one submission described advanced implementations that can be trained to recognize vocal biomarkers to assess for diseases or conditions by the altered sound of an individual's voice.

E. Education

Biometric technologies were touted in some RFI submissions in educational settings 1) to assess progress and detect plagiarism, 2) to increase student focus and engagement, and 3) for learning applications designed for students with disabilities. Respondents described proctoring and testing software that uses facial recognition to validate an individual's identity, which allows students to complete assignments and take tests remotely while maintaining the integrity of the distance learning environment. RFI submissions also described implementation of advanced systems capable of applying facial recognition in the classroom to analyze and review the engagement of students throughout a lesson to personalize knowledge content and delivery.

9. Governance Programs, Practices, or Procedures Applicable to the Context, Scope, and Data Use of Specific Use Cases

The RFI specifically aimed to solicit information related to governance programs, practices, or procedures applicable to the context, scope, and data use of specific use cases including information related to:[11]

1. 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;
2. Best practices or insights regarding the design and execution of pilots or trials to inform further policy developments;
3. Practices regarding data collection (including disclosure and consent), review, management (including data security and sharing), storage (including timeframes for holding data), and monitoring practices;
4. Safeguards or limitations regarding approved use (including policy and technical safeguards), and mechanisms for preventing unapproved use;
5. Performance auditing and post-deployment impact assessment (including benefits relative to current benchmarks and harms);
6. Practices regarding the use of biometric technologies in conjunction with other surveillance technologies (e.g., via record linkage);
7. Practices or precedents for the admissibility in court of biometric information generated or augmented by AI systems; and
8. Practices for public transparency regarding: Use (including notice of use), impacts, opportunities for contestation and for redress, as appropriate.

RFI respondents who addressed these points, directly or indirectly, frequently mentioned the need for oversight bodies and specific guidelines in a number of areas. Some organizations or groups called for a prohibition on specific types of uses of biometric data,

[11] Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies, 86 Federal Register 56,300 (October 8, 2021). https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies

while others volunteered that they declined to use biometric data for specific use cases where scientific support was lacking or where ethical challenges could potentially outstrip the benefits of use. Privacy laws at the international, State, and local levels were also mentioned by multiple respondents, with many emphasizing the need for legislation or guidance at the Federal level.

A. Oversight Bodies or Guidelines

Multiple respondents raised the need for guidelines regarding appropriate uses and use cases for biometric technologies and that such guidelines should include detailed information regarding management, retention, and maintenance of biometric data; unnecessary aggregation or retention of biometric data should be discouraged or prevented. Information regarding how human oversight should be integrated into the processes governing use of biometric technologies was mentioned in numerous RFI submissions. In addition, development of "regulatory sandboxes" to explore use-case feasibility in a safe environment was discussed by some respondents. The work being done by NIST to standardize and provide evaluation guidance was identified as valuable and helpful by many RFI submitters, although some specifically noted that NIST's work alone was insufficient to ensure safe and responsible use of biometric technologies.

A number of RFI respondents outlined practices they had voluntarily adopted to assess potential impacts, verify that benefits of specific use-cases outweighed potential risks, ensure privacy and accuracy, and prevent unapproved uses or applications of a particular product. Submissions addressing this subject varied extensively, with some organizations describing how they are attempting to specifically limit problematic or potentially high-risk aspects of biometric technologies, whereas others asked that no regulation, oversight, or auditing by third parties be imposed upon them. Regardless of whether RFI respondents expressed support for or opposition to stronger regulation and oversight, many requested that clear technical standards, guidelines, and oversight bodies should be developed and deployed to improve transparency, ensure that impact assessments are accurate, and hold institutions that employ biometric technologies accountable. The need for practices and oversight pertaining to use of biometric technologies in law enforcement were specifically mentioned by multiple respondents, as well as guidelines related to what types of biometric information should be admissible as evidence in legal proceedings.

B. Prohibition of Specific Use Cases

Numerous RFI responses advocated for prohibition of specific uses of biometric technologies—including mass surveillance, emotion detection, and social recommendations—because of the potential to perpetuate bias and injustice and a lack of scientific support for the accuracy of such biometric applications. Other respondents

argued that bans and moratoria effectively prevent development of appropriate regulation and stifle innovation in these areas. Instead, they argued that policies, requirements, and oversight may provide a path forward that allows implementers to document and evaluate key aspects of specific use-cases and allows regulators and implementers to work together to ensure biometric technologies are being used appropriately and responsibly.

C. Governance of Data and Privacy Protections

A number of respondents currently using biometric tools described best practices for handling and protecting sensitive biometric data, including enhancing privacy by default by blurring non-target faces when using facial recognition, discarding information from non-consenting individuals, controlling who within an organization has access to biometric data, and establishing clear data collection and retention limits and policies. Some organizations responding to the RFI also described policies and practices for retaining detailed records of actions taken in relation to biometric data to improve transparency and accountability—for example, logging and saving any actions to re-identify, delete, or otherwise alter biometric data. According to a number of respondents, informed consent is an area of concern that has not been sufficiently addressed by organizations that currently use biometric technologies. Some respondents also felt that data aggregation, including data sharing and aggregation by government agencies, is a danger to privacy and must be specifically addressed.

While some of these actions indicate that organizations are operating with intent to "do the right thing," many respondents expressed skepticism that this type of self-governance and internal monitoring is sufficient to safeguard against the potential risks that they feel biometric technologies pose. Submissions from some advocacy and civil liberties groups suggest that specific security standards, requirements for consent, and third-party oversight and auditing of biometric technologies should be implemented to ensure accountability and limit the potential harms associated with their use. Other RFI respondents suggested that promoting legal liability and accountability for privacy violations or inequitable or unsafe application of technologies will help to ensure proper assessments before new technologies are deployed.

D. Existing Standards, Laws, Frameworks, and Guidelines

Many respondents mentioned the General Data Protection Regulation (GDPR), which went into effect in the European Union in 2018, and the lack of equivalent protections for data and privacy in the United States. Submitters noted that in the absence of protections at the Federal level, many States and localities have passed their own laws to provide privacy or data protections or to govern the use of biometric-based technologies and applications. RFI respondents specifically identified adoption of some type of data or privacy protections at the State level in Illinois, Washington, Colorado, Virginia,

California, and Texas; at the city level, New York City, Portland, San Francisco, Oakland, and several municipalities in Massachusetts were noted to have laws regulating the use of biometric-based applications. Additional protections applying to information associated with individuals under the age of 13 (Children's Online Privacy Protection Act[12]) or medical data (Health Insurance Portability and Accountability Act[13]) were noted in several responses. Overall, many respondents voiced concern that the United States does not have a GDPR equivalent, and that State and local measures have resulted in a patchwork of regulations that may be difficult to track and comply with.

Multiple respondents indicated general support for use of biometric technologies, provided they are properly regulated and responsibly deployed; other RFI contributors expressed skepticism that regulation can be done in ways that are meaningful, with many cited examples of cases where law enforcement or other groups have skirted existing protections. Both implementers and other stakeholders suggested there should be regular monitoring of biometric technologies as long as they are in use, to ensure they maintain compliance with privacy, security, and other regulations over time. Some organizations suggested that guidance and oversight should be "technology neutral," while others suggested that medical and non-medical uses may need to be responsive to different types of regulation.

Finally, some respondents considered the unrestrained use of biometrics technologies in an international context and the impact that this could have on human rights globally if the United States and other countries do not begin to set cultural norms and standards for how biometric technologies can be deployed.

---

[12] Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506; https://www.law.cornell.edu/uscode/text/15/6501

[13] Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. § 1320d; https://www.law.cornell.edu/uscode/text/42/1320d

10. Recommendations Submitted to the Biometric RFI

In addition to providing perspectives and information to guide ongoing Federal policy discussions on the use of biometric technologies, RFI respondents made numerous recommendations for policies and actions as well as suggesting principles that should govern biometric policy making. Recommendations received from RFI submitters addressed many specific issues from numerous different points of view, but general concerns included:

- privacy and the ability of individuals to control access to and use of their biometric data;
- discriminatory bias in AI-powered biometric systems;
- chilling freedom of speech and association due to biometric surveillance;
- the security of sensitive biometric information; and
- defining clear boundaries on where, when, and how biometric technologies can be used.

In addition, respondents universally encouraged OSTP to continue to engage stakeholders—including developers and designers of AI technology as well as civil society advocates, private-sector users, and the general public—to develop voluntary standards, ethical guidelines, and best practices for testing, certification, and approved uses of biometric technologies.

A. Recommended Policy Principles

Although opinions were neither unanimous nor universal, RFI submitters expressed a number of principles to guide the formulation of policies governing biometric technologies:

- Give people ownership and agency over their own data as a fundamental right.
- Avoid bias and discrimination.
- Build on existing law and regulations governing non-discrimination, privacy, civil liberties, and human rights.
- Be evidence-based.

- Apply guidelines and regulations to well-defined use cases rather than focusing on specific technologies.
- Balance benefits and risks and particularly consider the elevated risks of vulnerable populations.
- Establish guardrails that promote innovation and prevent harmful use cases.

B. Recommended Federal Actions

Included in many Biometric RFI submissions were recommendations for Federal-level administrative or legislative actions:

- OSTP should establish an interagency task force on "Improving Digital Identity."
- OSTP should commit to research and policy proposals that center community- and justice-informed uses of algorithmic biometric systems.
- OSTP should not endorse any state-sponsored biometric tracking, storing, or sharing technologies or capabilities.
- OSTP should support Federal agencies in their efforts to better understand the use of automated systems in public benefits delivery and prohibit technology that marginalizes or harms communities entitled to benefits and care.
- OSTP should provide privacy standards to instruct both the public and private sectors on how biometric data should be handled and safeguarded.
- The U.S. Government should establish a single national governance and regulatory framework for biometric technologies.
- The U.S. Government should invest in development of a framework of standards and operating rules for biometric technologies in coordination with allied partner nations.
- The U.S. Government should promote beneficial uses of biometric technology.
- The U.S. Government should create safe and collaborative regulatory sandboxes as a means to develop and test policies for the use of biometric technologies.
- The U.S. Government should provide private companies access to government datasets to train biometric AI algorithms.
- The U.S. Government should establish a biometric data privacy framework using the NIST Privacy Framework as a guide.

- The U.S. Government should stay ahead of foreign actors and governments that attempt to leverage biometric technology for nefarious activities or to unfairly compete with the United States.
- The U.S. Government should regulate the export of biometric technologies by including them in the Department of Commerce's "dual use" control list.
- The Department of Education and the Federal Trade Commission should establish a working group to study the impact of biometric technology on children.
- Congress should enact legislation to address the indirect and disparate impact of AI-enabled biometric identification technologies in administering access to public and private services.

C. Recommended Bans, Prohibitions, and Moratoria

Some RFI submissions advocated outright bans, prohibitions, or moratoria:

- Ban the use of any biometric technology (including face, voice, and gait) for mass surveillance.
- Ban the use of facial recognition in a manner that could chill First Amendment activities or otherwise infringe on human or constitutional rights.
- Prohibit non-explicit consent for collecting or using biometric information.
- Prohibit the sale or transfer of biometric data to third parties.
- Suspend the use of facial recognition technologies in all circumstances known or reasonably foreseeable to be prejudicial to established human and legal rights.
- Ban the design, development, and use of biometric technologies for emotional or behavioral characterization.
- Ban automated gender recognition and AI-based "detection" of sexual orientation.
- Place a moratorium on all Federal Government use of facial recognition and other forms of biometric technology so long as discriminatory bias pervades these systems.
- Prohibit deployment of facial recognition technology prior to establishing appropriate policies governing its use and the management of data collected by the system.
- Ban the use of facial recognition in school settings.
- Ban voice and other forms of biometric profiling for marketing purposes.

- Place a moratorium on the use of mandatory AI-enabled biometric identification technology in critical sectors providing fundamental social services such as education, welfare benefits programs, and health care.
- Eliminate the use of biometric scanners at U.S. airports by the Transportation Security Administration.
- Ban the use of biometric technologies by law enforcement agencies.
- Prohibit local law enforcement agencies that receive Federal funding from maintaining their own DNA databases.
- Prohibit State and local governments from using Federal funds to purchase or access facial recognition technology.

D. Recommended Implementation Practices

RFI respondents made numerous recommendations on various aspects of the implementation of biometric technologies.

1. Consent

Opt-in/opt-out acceptances should be clear; non-explicit consent for use or sharing of images or other biometric data should not be allowed. If non-consensual uses of biomedical biometric data are permitted, they should ensure "public benefit."

2. Transparency

People should be informed using plain language when biometric tools are being used and for what purpose, particularly when monitoring individuals in public and private spaces and when biometric data are collected and used for commercial purposes. In the case of biometric data breaches, regulatory bodies and people who may be affected should be promptly informed.

3. Data

Data retention should be legally compliant, transparent to the public, limited to information that is strictly necessary for a specific purpose, and ended when the data are no longer needed. Data used to train AI-powered biometric technologies should be collected in a manner that does not violate the privacy of the data sources. Facial recognition systems should implement "obfuscation by default" to prevent capturing information on any person who is not specifically targeted for identity verification or recognition.

4. Security

Use of biometric technology for identity verification should be restricted to secure devices and require state-of-the-art encryption. Users and regulatory bodies should be informed of data breaches in a timely manner.

5. Accuracy

The magnitude and effects of a biometric system's biases and inaccuracies should be understood prior to deployment. When reported, error rates should be disaggregated by sex, race, and other context-appropriate demographic traits. Acceptable error rates should be defined by clear standards.

6. Audits

Biometric systems should be audited annually to test their effectiveness and identify inherent or emerging biases. Systems should retain a granular record of users and actions, and AI code should have a diagnostic toolkit embedded to detect biased outcomes. Biometric technology should be testable by certified, independent third parties.

7. Human Oversight

All AI facial recognition systems should have the capacity for manual correction and improvement, and no decisions affecting an individual's freedom or welfare should be made automatically without human oversight. All industries and research organizations engaging biometric data and inference systems should have a compensated advisory board of publicly listed members. Operators of facial recognition systems should receive mandatory training on their technical and ethical use.

8. Accountability

Standards for performance and testing (including the diversity of training data sets) should be established and enforced across the entire lifespan of a biometric system. Metrics should include fiscal and social risks as well as equity and inclusion. Violations of policies and laws governing privacy, equitability, and safety should incur appropriate penalties. Individuals should have clear mechanisms to redress grievances arising from errors and harm incurred from biometric systems.

E. Sector-Specific Recommendations

In addition to broadly applicable principles and recommendations, many RFI respondents made recommendations for policies in particular social or economic settings.

1. Biomedicine

Because biomedical records and information were recognized as a particularly sensitive form of biometric information, several RFI respondents recommended establishing guidelines for use of biometric technologies that could be linked to medical records. RFI respondents also addressed concerns about the use of genetic data to exclude vulnerable groups from services or employment and advocated that long-term care, disability insurance, and life insurance be added to the Genetic Information Nondiscrimination Act[14] to prevent health insurance companies and employers from discriminating based on genetic information. In addition to concerns about misuse of biometric information, RFI respondents also recognized the potential benefits and encouraged the expansion of using AI-based analysis of patient-generated health data in research, health administration and operations, public health, and direct clinical care.

2. Law Enforcement and Criminal Justice

Most RFI recommendations concerning the use of biometric systems in the arena of law enforcement and criminal justice focused on policies to prevent abuse and misuse of the technology. Many respondents argued that the use of biometric information should be limited to those cases where law or regulation requires it, or there is a clear value added to the community or to government operations. In particular, numerous RFI submitters recommended that facial recognition searches should require reasonable suspicion or probable cause, require a warrant, and be limited to the investigation of violent felonies. Respondents acknowledged that exemptions to limits on the use of biometric information could be necessary in emergencies, natural catastrophes, or cases where robust safeguards and regulations already exist. Numerous RFI respondents recommended that the use of facial recognition during an investigation should be disclosed to defendants as a matter of due process. Respondents also advised that investigative biometric technologies should meet the same standards of accuracy and reliability expected of any other form of court admissible evidence and should demonstrate their capacity for just and equitable application prior to their implementation in the criminal legal system. Submitters recommended that evaluations of the use of biometric technologies in the arena of law enforcement and criminal justice should be developed by a task force of technologists, racial justice experts, civil liberties experts, researchers, community members, and other criminal legal system stakeholders.

---

[14] Genetic Information Nondiscrimination Act of 2008 (GINA) Public Law 110-233: https://www.law.cornell.edu/wex/genetic_information_nondiscrimination_act_(gina)

3. Labor

A number of RFI respondents expressed concerns that AI-enabled biometric technologies could facilitate exploitative labor practices, especially for low-wage, disabled, or non-White workers. Although the need for more research was acknowledged, several RFI respondents recommended that the use of biometric technologies that can be reasonably construed to prohibit or diminish the exercise of labor rights by employees should be illegal.

4. Education and Children

Many RFI respondents expressed concern over the use of biometric technologies to monitor children in educational settings. Among the recommendations made in various RFI submissions were that biometric data should not be derived from students' social media and that facial recognition technology should not be used to monitor or police student behavior. In addition, respondents recommended that students' biometric data should be deleted at the end of each academic year, upon graduation, or departure from the district, whichever comes first. Outside of school, the value of AI-aided child sexual abuse detection methods was recognized in many RFI submissions and it was recommended that any proposed legislation or regulation should preserve the use of biometric technology in this context.

5. Public Benefits

Lastly, a number of RFI respondents addressed difficulties with the use of biometric technologies in the distribution of public services and recommended that biometrics should be limited to identity verification (one-to-one) rather than to identification (one-to-many).

Abbreviations

AI	Artificial intelligence
FERPA	Federal Educational Rights and Privacy Act
GDPR	General Data Protection Regulation
GINA	Genetic Information Nondiscrimination Act
HIPAA	Health Insurance Portability and Accountability Act
NIST	National Institute of Standard and Technology
OSTP	Office of Science and Technology Policy
RFI	Request for Information
STPI	Science and Technology Policy Institute

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
XX-03-2022	FINAL	

4. TITLE AND SUBTITLE

Synopsis of Responses to OSTP's Request for Information on the Use and Governance of Biometric Technologies in the Public and Private Sectors

5a. CONTRACT NUMBER

NSFOIA-0408601

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Olszewski, Thomas D.
Van Pay, Lisa M.
Ortiz, Javier F.
Swiersz, Sarah E.
Dacus, Laurie A.

5d. PROJECT NUMBER

TP-20-1005.DH

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IDA Science and Technology Policy Institute
1701 Pennsylvania Avenue, NW, Suite 500
Washington, DC 20006-5805

8. PERFORMING ORGANIZATION REPORT NUMBER

IDA Document D-33070

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue, NW
Washington, DC 20504

10. SPONSOR/MONITOR'S ACRONYM(S)

OSTP

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited (13 April 2022).

13. SUPPLEMENTARY NOTES

14. ABSTRACT

On October 8, 2021, the Office of Science and Technology Policy (OSTP) posted a Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies. The purpose of the RFI was "to understand the extent and variety of biometric technologies in past, current, or planned use; the domains in which these technologies are being used; the entities making use of them; current principles, practices, or policies governing their use; and the stakeholders that are, or may be, impacted by their use or regulation." In conjunction with the RFI, OSTP also hosted two public listening sessions (November 18 and 29, 2021) for individuals to share oral comments. This report provides the Science and Technology Policy Institute's synopsis of both oral comments expressed in the listening sessions and written responses submitted to the RFI.

15. SUBJECT TERMS

biometric; biometric technology; Request For Information (RFI)

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Marda, Nikhil
Unclassified	Unclassified	Unclassified	Same as Report	42	19b. TELEPHONE NUMBER *(Include area code)* Nikhil.R.Marda@ostp.eop.gov

Reset

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18