This document is scheduled to be published in the
Federal Register on 10/08/2021 and available online at
federalregister.gov/d/2021-21975, and on **govinfo.gov**

OFFICE OF SCIENCE AND TECHNOLOGY POLICY

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

AGENCY: Office of Science and Technology Policy (OSTP).

SUMMARY: The Office of Science and Technology Policy (OSTP) requests input from interested parties on past deployments, proposals, pilots, or trials, and current use of biometric technologies for the purposes of *identity verification*, *identification of individuals*, and *inference of attributes including individual mental and emotional states*. The purpose of this RFI is 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. OSTP encourages input on both public and private sector use cases.

DATES: Interested persons and organizations are invited to submit comments on or before 5:00 p.m. ET on January 15, 2022.

ADDRESSES: Interested individuals and organizations should submit comments electronically to BiometricRFI@ostp.eop.gov and include <*RFI Response: Biometric Technologies*> in the subject line of the email. Due to time constraints, mailed paper submissions will not be accepted, and electronic submissions received after the deadline cannot be ensured to be incorporated or taken into consideration.

Instructions:

Response to this RFI is voluntary. Each responding entity (individual or organization) is requested to submit only one response. OSTP welcomes any responses to help inform policies, especially those with a view toward equitably harnessing the benefits of scientifically valid technologies approved for appropriate contexts with iterative safeguards against anticipated and unanticipated misuse or harms.

Please feel free to respond to one or as many topics as you choose, while noting the number of the topic(s) to which you are responding. Submission must not exceed 10 pages in 12-point or larger font, with a page number provided on each page. Responses should include the name of the person(s) or organization(s) filing the comment, as well as the respondent type (e.g., academic institution, advocacy group, professional society, community-based organization, industry, member of the public, government, other). Respondent's role in the organization may also be provided (e.g., researcher, administrator, student, program manager, journalist) on a voluntary basis. Comments containing references, studies, research, and other empirical data that are not widely published should include copies or electronic links of the referenced materials. No business proprietary information, copyrighted information, or personally identifiable information should be submitted in response to this RFI. Please be aware that comments submitted in response to this RFI may be posted on OSTP's website or otherwise released publicly.

In accordance with Federal Acquisitions Regulations Systems 15.202(3), responses to this notice are not offers and cannot be accepted by the Federal Government to form a binding contract. Additionally, those submitting responses are solely responsible for all expenses associated with response preparation.

FOR FURTHER INFORMATION CONTACT: For additional information, please direct questions to Suresh Venkatasubramanian at biometric@ostp.eop.gov.

SUPPLEMENTARY INFORMATION: *Background:* To date, attention and legislation around AI-enabled biometric technologies has largely focused on the specific case of facial recognition technology used to identify individuals in law enforcement and in public and private settings. However, there are a growing number of domains that are beginning to make use of biometric information for *identification* or *inference* of emotion, disposition, character, or intent. This expanded set of uses includes but is not limited to:

- The use of facial recognition to control initial and continuing access to resources such as housing, medical records, schools, workplaces, and public benefits;
- Facial or voice analysis in employment (e.g., to screen potential hires for trustworthiness and competence), education (e.g., to detect risks to safety, determine student focus and attention in the classroom, and monitor online exams), and advertising (e.g., to determine responses to advertising displays or track behavior in physical shopping contexts);
- Keystroke analysis for detection of medical conditions and cognition or mood;
- The use of gait recognition, voice recognition, and heart rate analysis for inference of level of cognitive ability and performance in healthcare (e.g., for stroke recovery, and aids for autistic individuals); and
- Inferring intent (and mal-intent) in public settings.

Many concerns have been raised about the use of biometric technology, ranging from questions about the validity of the underlying science; differential effectiveness, outcomes, and harms for different demographic groups; and the role of biometric systems in increasing the use of surveillance technologies and broadening the scope of surveillance practices. Nonetheless, biometric technologies are often presented as a cheaper and more reliable form of identification, and as effective aids in clinical settings for diagnosis and therapeutic use, in addition to their use in public safety such as for finding missing persons and combating child trafficking.

OSTP seeks information and comments about AI-enabled biometric technology uses, including but not exclusive to the above.

Terminology: We use "biometric information" to refer 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. For the purpose of this RFI, we are especially interested in the use of biometric information for:

- **Recognition.** This includes the use of biometric information for *verification* (matching a claimed identity to a reference identity) and *identification* (real-time or post-facto identification of an individual or of all individuals in a crowd either in pursuit of a legal case or as part of broad surveillance in varied domains); and
- **Inference of cognitive and/or emotional state.** This includes the use of biometric information for *inference* of cognitive and/or emotional states (such as attentiveness, mental fatigue, stress, anxiousness, fear, or cheerfulness).

We broadly refer to a system that uses biometric information for the purpose of recognition or inference as "biometric technology."

Scope: OSTP invites input from any interested stakeholders, including industry and industry association groups; civil society and advocacy groups; state, local, and tribal governments; academic researchers; technical practitioners specializing in AI and biometrics; and the general public. In particular, OSTP is especially interested in input from parties developing biometric technologies, parties acquiring and using such technologies, and communities impacted by their use. Input is welcome from stakeholders, including members of the public, representing all backgrounds and perspectives.

Information Requested:

Respondents may provide information for one or as many topics below as they choose. Through this RFI, OSTP seeks information on the use of biometric technologies in the public and private sectors, including on the following topics:

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.

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.
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.
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.

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

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

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

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

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

    f. Practices regarding the use of biometric technologies in conjunction with other surveillance technologies (e.g., via record linkage);

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

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

Please note any governance measures that are required by law or by government, including human or civil rights frameworks, or corporate policy, including ethical principles, in cases of deployment, as well as any planned governance measures for planned or current-use biometric technologies.

Dated: October 4, 2021.

Stacy Murphy,

Operations Manager.

[FR Doc. 2021-21975 Filed: 10/7/2021 8:45 am; Publication Date: 10/8/2021]