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

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

November 17, 2021  

Dear Suresh Venkatasubramanian,  

Thank you for the opportunity to respond to the “Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies.” Our comments are primarily focused on “(6) Governance programs, practices or procedures applicable to the context, scope, and data use of a specific use case” from the federal register posting, although we may touch on several points related to other areas of comment.

Palantir Technologies, Inc. (“Palantir”) is a U.S.-headquartered software company. We provide enterprise data platforms that enable public and private institutions to integrate, analyze, collaborate, and take action based on their data in a privacy-protective way. We have over 15 years’ experience working with governments and commercial organizations on sensitive problems including in areas relevant for this RFI. Our technology is meant to reconcile the need for security with the value of privacy and we reject the notion that there is an inherent tradeoff between security and privacy. Our goal in responding to this RFI is to share best practices we have developed to inform future regulation.

Unlike many tech companies, we do not collect, store, disseminate, sell, or otherwise monetize customer data. We make software to help some of the most critical organizations around the world to make better use of the data they already lawfully possess or access.

Palantir operates on the conviction that it is essential to preserve fundamental principles of privacy and civil liberties while using data. We believe that well-designed technologies can dramatically enhance security without undermining the rights and freedoms of individuals. Our work strengthens national security while supporting constitutional privacy protections.

Upholding these principles means integrating new technologies for processing data responsibly. Our experience working with a broad range of public and private sector organizations has continually reinforced our position that there are both responsible and irresponsible ways of using sensitive data and algorithms. This insight applies as well to biometrics and facial recognition.

To be clear, Palantir does not collect or hold facial recognition data, it does not build facial recognition algorithms, nor does it hold any direct stake in the adoption of this technology. To the contrary, we believe that there should be limits placed on the use of such powerful technologies, including restrictions on their use for programs that could be construed as mass surveillance. Narrowly circumscribed applications based on appropriate legal authorities and integrating critical privacy-preserving safeguards may present more defensible use cases. As a company that provides data integration platforms, we view facial recognition data as one of several sensitive classes of biometrics data that may — under the right conditions and with appropriate controls — be used in direct, stand-alone form or as integrated into a more...
generalized information or analytics environment. In either case, we believe technological capabilities coupled with procedural controls show that a more prescriptive approach to facial recognition regulation can achieve both security and privacy goals. We believe that sharing these principles and best practices will help empower organizations and regulators to effectively regulate facial recognition technologies.

The suggestions included in this document are primarily intended to apply to the use of facial recognition systems for specific security applications, but many of the same ideas may apply to other potential uses of facial recognition and even other biometric technology applications. That said, a critical consideration to call attention to up front is that determining the appropriateness of facial recognition use is indeed a context-dependent exercise and requires a concrete outline of the conditions of use in order to make a clearer assessment of the attendant privacy and civil liberties risks, as well as adequacy of mitigating measures.

**Recommendations**

**Limiting Facial Recognition Technologies**

This submission proposes principles that impose technological limitations for facial recognition systems used for security provision. We believe that policies can direct the intelligent design and application of these systems to capture the essential security utility of facial recognition technologies whilst achieving what we term *engineered ephemerality*. That is the notion that non-suspect individuals should be able to pass by facial recognition systems with minimal consequence or no trace at all.

By ‘facial recognition technologies’ we refer to those systems that attempt to

- a) detect human faces that appear in still imagery and video footage
- b) attempt to derive the unique geometry of detected faces
- c) match derived facial geometric data against previously obtained target data held within databases.

Though there may be other operational definitions of facial recognition technologies, we believe this definition will cover the majority of applications in the security context.

Technical measures alone are insufficient to ensure the safe use of facial recognition technologies. The measures suggested here are intended to compliment, not replace, governance mechanisms such as limiting the purposes for which such technologies can be employed, establishing oversight bodies, and acting transparently to ensure that the affected public is informed about programs and environments using facial recognition systems.

We are primarily responding to the use of Facial Recognition for use in the physical security of a sensitive facility or at an international border crossing. By contrast, we do not believe that indiscriminate use in contexts that could construed as mass surveillance, even if all these guidelines are followed, would be justifiable or warranted.

In addition, we advise heavy skepticism with regards to the use of biometric technology, including processing of facial features, in systems that purport to identify a person’s interior
states, such as their emotions, thoughts, or intentions, as well as its use in job hiring or other social recommendation scenarios.

**Obfuscation By Default**

Facial recognition technologies present a challenge to ‘practical obscurity’ as a traditional privacy protection. In the absence of machine-assistance, facial detections are the product of human observations and cognitive faculties with all the benefits and limitations of vision, memory, attention, etc. Facial recognition technologies enable augmented or fully automated detection and identification of faces. While for certain institutions, the prospect of more expansive surveillance can foster valuable security protections, an uninhibited approach can lead to significant and alarming privacy intrusions.

Facial recognition systems can, however, be engineered and configured to mitigate privacy concerns by using the same technology that enables facial detection to automatically obfuscate or blur detected faces to system users.

We propose that facial recognition systems should implement an ‘obfuscation by default’ paradigm that obfuscates (blurs) imagery exposed to end users for both unidentified faces and known faces that do not trigger an alert or other appropriate viewing threshold. In other words, unless there is a reason, faces should not be visible to system users. When there is a reason to allow viewing of faces, authorized users should operate under proportionately granted, auditable access controls that limit viewing of faces in an appropriate way.

Obfuscation by default ensures that any imposition on privacy is appropriately proportionate with the end-users’ authorized objectives while minimizing casual browsing of imagery and potential privacy intrusions. Faces that require identification as a legitimate part of a security investigation or other appropriate use case could be unmasked by an explicit user action with associated reason justification recorded (more on this below).

**Limiting data collection**

In one of the most common applications, facial recognition systems attempt to match the facial geometry of newly encountered individuals against previously collected facial geometry data stored within databases. We term the list of individuals whose facial geometry data populates these databases *seed lists*. Management of seed lists must be robust. That is, the objective should be to keep these lists as short, current, and reliable as possible, proportionate to legitimate security needs.

The addition of data to, or the removal of data from, seed lists should require and document explicit justifications. Seed list alterations and their associated justifications should follow an established policy and be subject to oversight.

Seed lists should be subject to mandatory review and reconfirmation of their ‘membership’ at reasonable and regular intervals. We suggest that every six-months is a reasonable schedule for these reviews (though alternative retention periods may apply, depending on the context).
default assumption for these reviews should be that, unless specific evidence justifies the continuing inclusion of an individual on a seed list, the individual should be removed.

**Limiting Data Retention**

Ensuring that data generated by facial recognition systems is deleted after an appropriate period of time is essential to achieving ‘engineered ephemerality’.

If a facial recognition system encounters an unknown face (a face that does not match any of those in relevant seed lists), then biometric data concerning this unknown face should be subject to limited retention or immediate deletion. This prevents unnecessary data aggregation on non-suspect individuals, allowing them to pass by facial recognition systems leaving minimal or no trace.

If a facial recognition system returns a match against an individual on a seed list, then a record of this match (including metadata such as time and location) should be made and stored for a moderate period. We suggest that one month would be a reasonable default retention period for this set of records. During this period, human analysts can review the possible match to determine if it was accurate and significant.

If a match passes these checks, then it can be elevated to a third, longer retention category. The retention period of this category should not be unlimited but should be calibrated with reference to the laws and best practices relevant to the defined mission that the data is intended to serve.

**Limiting System and Data Access**

Access to the processes and data of facial recognition systems should be governed by granular access controls. This means that users should be able to discover, view, process, edit, and delete sensitive data only to the extent that their responsibilities and roles demand. Data from video capture and facial recognition technologies should not be available indiscriminately across an organization.

Granular permissions preventing unauthorized access should be applied to all levels of system interaction, including but not limited to:

- Viewing the imagery that facial recognition systems analyze (e.g., CCTV feeds)
- Viewing seed lists
- Editing seed lists
- Viewing facial recognition matches
- Viewing maps and schematics identifying location of facial recognition capture devices
- Deleting system data
- Escalating retention periods
- Viewing audit logs
Selective Revelation with Purpose Justifications

Facial recognition systems should include mandatory documentation of user justifications for key actions undertaken, including but not necessarily limited to:

- De-obfuscating an obfuscated (i.e., blurred) facial image or detection
- Adding data to a seed list
- Removing data from a seed list
- Extending retention periods for data within a seed list
- Ad-hoc searches against a facial geometry database
- Exporting data

Justifications provided by users can take multiple forms, but we recommend pre-determined justification categories formulated with the support and review of appropriate oversight authorities and codified in system usage policies and guidelines. In other applications, it may be appropriate for users to provide case number or other critical reference details in addition to or in lieu of category or free-form text justifications.

Facilitating Oversight

A thorough audit log of all significant user actions within the system should be maintained. This allows those responsible for system oversight to detect and investigate illegitimate user behavior and to hold users accountable for actions undertaken within the system.

Audit logging capabilities should be sufficiently detailed and accessible to determine whether individuals are misusing data by inappropriately accessing information, conducting overly-broad searches, deliberately or inadvertently entering erroneous information, sharing or exporting information without authorization, or engaging in other activities that could lead to serious violations of privacy and civil liberties.

At a minimum, audit logs should include details regarding the specific user, user action in the system, corresponding metadata (e.g., date/time), data elements the user action exposes or interacts with, and (where appropriate) justifications provided by users to carry out specific actions.

Audit log analysis applications for the facial recognition system used in this example physical security context should be developed and made available to oversight bodies that allow these bodies to identify inappropriate use, analyze audit logs at scale, and highlight anomalous or concerning behavior. Raw and uninterpretable logs will not allow oversight bodies to protect civil liberties in the proper context.

Data and Algorithmic Quality

The history of facial recognition systems is rife with examples of applications beset by poor accuracy and systemic unfairness. These outcomes are unacceptable. Proper control over facial
recognition use is not sufficient if the facial recognition systems themselves have or propagate unwanted biases.

Evaluations of algorithmic performance across a range of different identity groups, demographic backgrounds, dress conditions, disabilities, and other physical variations must be conducted before a facial recognition system goes live, as well as continuously throughout the lifecycle of the system. Test images should be representative of actual deployment scenarios including lighting, camera placement, and image quality. Minimum acceptable standards should be established in advance, and these standards should accord with the potential for harm resulting from false-positives in any given use case.

When a system returns a match, it should also return a well-specified ‘confidence score’ assessment that conveys the confidence the system has that this match is not a false-positive.¹ This match should be visually apparent and prominently displayed to the end-user. If the confidence score does not meet a defined threshold, then the image match should not be displayed to end-users.

Systems should have an embedded capacity for manual correction and improvement. When an end-user identifies a false-positive or a false-negative, the system should allow the end-user to correct such high-impact errors. In the case of a false-positive, the correction should remove the association between the falsely matched person (or object, if the system has identified a non-human entity as a face) and the video footage. All corrections should be clearly recorded in the audit log. Corrections may also feed back into the underlying facial recognition software to improve training and reduce error rates over time as well as flag disparate impact on an impacted population.

**Training data oversight**

Data used to train facial recognition algorithms, as well as data used to test those algorithms’ efficacy in potential application scenarios, should be collected according to principles of transparency and explicit consent of the individuals represented by the data. More directly, implied or non-explicit consent (e.g., opt-out requests buried deep in the bowels of Terms and Conditions should not be allowed). Similarly, images captured and tagged for one consented use should not be freely repurposed for the development or training of facial recognition algorithms or systems without additional explicit consent from subjects of the images.

¹ Confidence Score’ is intentionally under-defined. We leave it as a matter for later, context-specific determinations about the question of how confidence scores are designated, recognizing that there are a plethora of facial recognition evaluation metrics and algorithm evaluation standards that have been elsewhere articulated and that can be used individually or in composite form for “confidence” representations along the above lines. The critical points here are that a) confidence scores should be defined and agreed upon by appropriate oversight authorities, b) how those scores are defined and were determined as the appropriate metrics should be plainly documented, c) scores should be evaluated and consistently displayed in practice and in regular system use.
Preserving the Role of Human Judgement

Finally, decisions that can impact an individual’s freedom should not be left to exclusively to software. Facial recognition systems and processes should be designed to augment rather than replace the decision-making capability of human analysts. A human capable of spotting false-positive matches should be the decision-making endpoint in any facial recognition-facilitated operation. Analysts should undergo training to allow them to better understand the weaknesses of automated systems (as well as their own inherent biases) to identify errors, the role of both human and system bias, and to interact with the system in a responsible way.

Conclusion

Facial recognition has great potential for enabling meaningful and constructive security outcomes but must be evaluated against privacy and other social costs attendant to its use. We firmly believe that better security that leverages facial recognition and other biometric technologies need not come at the expense of privacy and civil liberties. This submission proposes several technical and administrative limits on facial recognition systems used for security. We assert that these limits are feasible and should be considered as part of future regulation. We welcome further discussion with OSTP on this proposal.

Sincerely,

Anthony Bak, Head of AI Implementation, Palantir Technologies
Courtney Bowman, Global Privacy and Civil Liberties Lead, Palantir Technologies