Response to Request for Information:
Public and Private Sector Uses of Biometric Technologies
86 Fed. Reg. 56300 (Oct. 8, 2021)

January 14, 2022

Google strives to make the technology we develop human-centered, accurate, fair, secure, based on sound science, accountable to people and, ultimately, a benefit to society. Google welcomes this opportunity to provide comments in response to the White House Office of Science and Technology Policy (OSTP) Request for Information (RFI) on biometric technologies.[1]

The development and use of biometric technologies in a variety of applications in the public and private sectors – and our collective understanding of the benefits and risks for individuals, communities, and society more broadly – has rapidly expanded in recent years. We agree with OSTP that it is timely and important to examine which classifications and applications of biometric technologies can be used responsibly to enable useful, secure, personalized, and accessible products and services that guard against harmful outcomes. In parallel, it is important to examine how best to protect against misuse and abuse, such as mass surveillance of individuals, particularly without their awareness or consent, in a manner that infringes on human rights and civil liberties.

Our comments focus on how OSTP can help foster the responsible development and use of biometric technologies. Terminology around biometric technologies is varied; to provide clarity, we define and assess the biometric techniques identified in the RFI and provide examples of how Google employs these techniques in our products and services. Our comments also speak to the risks and benefits of the development and use of the techniques and the mitigations we put in place.

Google believes any governance framework for biometric technologies should be proportional and enable a holistic examination of the technologies employed. It should also recognize that not all techniques or use cases are equally able to anticipate the specific use cases to which they are applied. To that end, our comments describe the principles and practices Google considers core to the responsible development and use of biometric technologies, including those reflected in our AI Principles[2], Privacy

[1] 86 Fed. Reg. 56300 (Oct. 8, 2021).
[2] https://ai.google/principles/

and Security Principles[3], and Human Rights Program[4] which guide our careful approach. We also suggest factors for consideration in developing a governance framework, including any regulatory treatment.

We welcome the opportunity to engage further on these issues with OSTP and other stakeholders, and expand on the issues covered in these comments.

Biometric technologies that identify individuals: Authentication and Identification

Biometric technologies identify specific individuals based on their biological characteristics (*e.g.*, face, iris) and/or behavioral traits (*e.g.*, gait).[5] They can be divided into two general categories of applications: authentication and identification.

Biometric "authentication": Biometric authentication involves comparing an individual's biometric data, such as a fingerprint, to a template or trusted identity document. The goal is to determine whether they match to verify the identity of an individual (*e.g.*, to provide access to a secure location or device). Many people embrace biometric authentication (*e.g.*, voice, fingerprint) because it is simple; biometric identifiers cannot easily be lost, forgotten, or stolen; and they can be combined with traditional password and PIN methods for even greater security and accountability.[6]

Biometric "identification"**:** Biometric identification involves searching a database of biometric identifiers for a match with the identifier of a specific individual.[7] Biometric identification enables a variety of beneficial features and personalized experiences for users, and there are a number of safeguards that can be put in place to manage risk. But certain biometric identification technologies like facial recognition can also be used in high-risk applications, for example for mass surveillance. Google has taken a cautious approach[8] to these technologies, and they are deployed in a small number of Google products with specific provisions guiding their application in areas where we have identified beneficial uses.

Biometric authentication and identification systems are used in a variety of Google products. For example:

- *Pixel Unlock:* Users can opt to set up fingerprint recognition to unlock Pixel phones, by providing a series of differently angled fingerprints which are used to create a model of the fingerprint belonging to the phone's owner. When

[3] https://safety.google/principles/
[4] https://about.google/human-rights/
[5] *See, e.g.*, ISO/IEC TR 24741:2018(en), Information technology — Biometrics — Overview and application.
[6] https://www.gartner.com/smarterwithgartner/the-iam-leaders-guide-to-biometric-authentication
[7] *See, e.g.*, ISO/IEC TR 24741:2018(en), Information technology — Biometrics — Overview and application.
[8] https://ai.google/responsibilities/facial-recognition/

someone tries to use the phone, the system can compare that person's fingerprint against the enrolled model, keeping malicious actors out while allowing users to unlock their device with a single touch.

- *Unlocking Incognito Tabs:* With the Chrome 92[9] update for the iOS version of Chrome, users can optionally secure incognito browser tabs to only be unlocked with Touch ID, Face ID, or a passcode. To enable this, just as for Pixel Unlock, users provide samples (either fingerprints or face images), which are used to create a model of the authorized user on the device.

- *Confirming credit cards with biometrics:* Users that choose to save credit card information to their Google account can enroll to retrieve that information via biometric authentication stored on the device, such as fingerprint or face verification.

- *Face Match on Nest Hub Max:* Face Match uses facial recognition to allow multiple people in a home to get personalized help on a shared home device – from seeing their personalized calendars and morning commute details, to checking missed messages meant just for them, or even playing their own favorite song. For each person who opts in to Face Match, the Assistant guides them through the process of creating a face model, which is encrypted and stored on the device. Following setup, all face matching occurs locally on the device. The user remains in control all the time and can opt-out of the feature and delete their face data at any time.

- *Nest Familiar Face Detection:* Users can opt in to use the Familiar Faces feature on Nest Cameras with a Nest Aware subscription (in compliance with the law). When a Nest Cam detects a face, the Familiar Faces feature allows a user to teach their camera whether that face is a known or unknown person. The user can assign known individuals names, and opt to receive notifications when these known individuals are detected by the camera on their property. The user remains in control at all times and can opt-out of the feature and delete their face library at any time.

- *Cloud Celebrity Recognition API:* Google Cloud offers a celebrity recognition API to authorized media and entertainment companies, helping them to identify a limited number of commonly recognizable celebrities in professionally produced media content. We have defined service specific terms[10] that apply to all users of the API and the API is only available by application only to media & entertainment customers with use cases that align with our terms of service.

[9] https://chromium.googlesource.com/chromium/src/+/e567a85af0255a6d759fb11bf07576d95345df0b
[10] https://cloud.google.com/vision/docs/celebrity-recognition

Applications that do not identify individuals: Detection, Clustering, Inference and Tracking

There are also applications that may involve processing biological characteristics, but not with the purpose of identifying specific individuals. These applications often involve fewer risks to individual rights and privacy than those associated with systems that identify individuals. While there are still risks associated with these applications (as outlined in the next section), the addition of identification heightens those risks. Applications which do not identify individuals, but process biological characteristics to deliver beneficial functions that would not otherwise be possible, are an area where innovation should be encouraged.

Detection: Allows a system to discern the presence and location of humans or particular body parts (*e.g.*, faces) in images or videos.[11] This technology can help computers answer questions like "where are the hands in this image?" or "how many faces are there in this image?" Detection is used in products like the Google Pixel camera to unblur faces.[12]

Clustering: A method that groups faces or other objects in images and video by likeness. Clustering is used in products like Google Photos to help users search and label their pictures by grouping pictures that include the same person.[13]

Inference: The process of drawing conclusions regarding a person's characteristics using physiological or behavioral information. This process would include, for example, providing suggestions for improved wellness based on data from sensors or trying to improve communication through interpretation of facial or vocal expressions. For example, an accessibility feature in beta in Android 12 allows users to control their phones with facial expressions, helping users who have difficulty with touch or voice controls more easily use their phones.[14]

Tracking: Identifies distinct attributes of an individual, but not who that individual is, allowing them to be tracked as they move through a space and are picked up on different sensors, such as through different video frames. Tracking can help computers answer questions like "what path do customers follow through this store," but not who those specific customers are, to help with product placement and identify areas of frequent congestion.

---

[11] Object Detection in 2021: The Definitive Guide, available at https://viso.ai/deep-learning/object-detection/

[12] https://www.androidcentral.com/how-does-face-unblur-feature-work-google-pixel

[13] https://support.google.com/photos/answer/6128838?hl=en&co=GENIE.Platform=Android

[14] https://www.theverge.com/2021/8/16/22626754/android-accessibility-face-gesture-controls

Responsible development of technologies that use biological characteristics

Technologies that use biological characteristics to identify individuals or to infer emotion, disposition, character, or intent (as outlined in the RFI) carry a wide array of potential benefits and risks – some linked to features of the technology itself; others arising from how the technology is used. For example, face detection can be used to help cameras take better photos by improving focus on faces, but it may not work equally well for all skin tones and thus create or exacerbate inequities.[15] Similarly, inference technology can help people who are blind or low-vision to read facial expressions, or help those with neurodiverse conditions (*e.g.*, autism) learn to better recognize different human emotional expressions. However, using such technologies to attempt to infer criminal intent (*e.g.*, based on an individual's facial expressions or voice characteristics) may lead to unfair interventions or create escalation dynamics that lead to harm. It is thus important to consider both the technology and the specific use case or application when assessing risk.

Google is very careful about deploying biometric identification in products and services because they come with heightened risk. Potential risks include performance and fairness issues (*e.g.*, lower accuracy across different genders, skin tones, ages); privacy and security risks to users' information being exposed (*e.g.*, voice, fingerprints); and sensitive use cases (*e.g.*, when identification is combined with tracking, it can be used to surveil individuals' movements over time, while identification and inference could be used to profile individuals' preferences and private thoughts in ways that violate their privacy). These risks can lead to serious harms. For example, false matches can lead to individuals being incorrectly accused of crimes, and non-matches can lead to denial of services.

While each biometric technology application is distinct and context specific, there are some generalizable responsible practices in line with our AI Principles and Privacy and Security Principles.[16] In summary:

- The application must be likely to deliver significant, concrete overall benefit to users and customers. Likely benefits should be verified through extensive user testing, including testing to determine whether any groups have been negatively affected in consultation with experts in machine learning fairness and internal stakeholders;

- Data used for model development, training, and evaluation should be appropriately licensed or otherwise approved for the intended use. Similarly, appropriate notice and consent mechanisms must be in place for collection and use of user data by the application;

[15] https://modelcards.withgoogle.com/face-detection

[16] https://ai.google/principles/ and https://safety.google/principles/

- Unless there is a critical product need, or reasonable expectation on behalf of users that biometric data will be stored, it should be immediately processed and not stored at all. If biometric data is to be stored, it should be in line with best practices and legal requirements (*e.g.*, deleted or obscured within a defined number of days where appropriate; safeguards in place to prevent misuse).

For more established forms of biometric applications, such as face-related technologies, we provide more specific guidance to product teams in the form of internally tailored questions and recommendations. Such frameworks are intended to be living documents, which can be updated as needed to account for evolving technology and changes to government policies.

Another responsible practice is to consult with relevant experts in communities that may be impacted by these technologies. For example, in 2018 Google commissioned BSR (Business for Social Responsibility) to conduct a human rights impact assessment of facial recognition technologies based on the UN Guiding Principles on Business and Human Rights. The assessment included a review of existing literature in the space and consultations with potentially affected stakeholders and independent experts. While we identified potential benefits – including business benefits – of certain specific applications of facial recognition, we ultimately determined that we would not offer general-purpose facial recognition APIs before working through key technology and policy questions.[17] Instead, we advised our product teams to concentrate on narrowly focused solutions, and enacted several safeguards to ensure the responsible development and use of tailored applications. For example, we developed a Celebrity Recognition API (noted above) which allow-lists companies for access and includes an opt-out policy for celebrities to request removal from the system.[18]

There also are heightened security risks posed by biometric identification technologies. Because an individual's biometric data (*e.g.*, fingerprints, DNA, vein patterns) cannot typically be changed if compromised, they are high value targets for bad actors. As such, companies that collect and process biometric data need to implement appropriate safeguards to protect against data breaches. For Android, we maintain an open source Measuring Biometric Unlock Security[19] resource to help our partners ensure the security of biometric data across services and devices. This includes guidance on architectural security, biometric security performance, and related metrics like imposter acceptance rate (the chance someone mimicking a legitimate input can deliberately fool the model), and false acceptance rate (the chance the model will accept a randomly chosen input).

Because biometric recognition technologies are based on biological characteristics, variations in characteristics across different groups of users can lead to differences in

[17] https://cloud.google.com/blog/products/ai-machine-learning/celebrity-recognition-now-available-to-approved-media-entertainment-customers

[18] https://cloud.google.com/vision/docs/celebrity-recognition

[19] https://source.android.com/security/biometric/measure

performance. To address this risk on Android devices, for example, Google calibrates presentation attacks[20] across a variety of faces to maximize the chances of uncovering performance gaps. Testing biometric authentication mechanisms in this way helps to reveal substantially poorer performance for segments of the global population, thereby helping Google ensure that these models function fairly and equitably across different demographics. Google employs a similar approach for its fingerprint recognition technology, using a variety of fingerprints to determine the optimal parameters for recognition and spoof testing.

Recommendations to OSTP

Technologies that use biological characteristics create beneficial new capabilities and offer personalized experiences for users. Any framework for biometrics should take a risk-based approach, enabling beneficial innovation in lower-risk applications while promoting effective protections for certain high-risk technologies and applications. Because biometric recognition technologies can pose a higher risk of harm to individuals, communities, and society, it is appropriate that they incorporate more rigorous safeguards. Furthermore, frameworks governing biometric technologies should provide clear guidance and resources to deployers of biometric identification systems. This could include, for example, recommended practices for receiving and responding to user feedback, and a library of techniques for measuring the accuracy[21] of biometric identification systems, including benchmarks of minimum sample sizes for determining error rates and standards for performance testing across different user attributes - such as gender, skin tone, voice or region - as relevant to a given technology.

To assess potential risks, the framework should take into account both technical features and the application or use case of a biometric system, including how people interact with and interpret the outputs of the system. This includes factors like accuracy, latency, the benefits and drawbacks of cloud versus on-device biometrics processing,[22] the likelihood of malicious attack or attempted deception, and the impact of any successful attacks. It also includes whether the system is used to, for example, authenticate users for secure device access or to identify individuals passing through a building. The framework could also provide guidance on factors to consider when determining appropriate safeguards against both anticipated and unanticipated

[20] A presentation attack is the presentation of an artifact or human characteristic to the biometric capture subsystem in a fashion that could interfere with the intended function of the biometric system. *See* Evaluation of Presentation Attack Detection: An Example, NIST available at https://www.nist.gov/system/files/documents/2020/11/04/15_tuesday_johnson_evaluation_of_presentation_attack_detection_an_example_ibpc2014_sacs2.pdf

[21] Accuracy refers to the frequency with which biometric signals are matched with the correct individuals. Certain biometric technologies offer higher accuracy than others, for example, DNA and fingerprint biometrics generally offer a higher level of accuracy than face or palm print biometrics.

[22] For example, on-device processing may provide greater privacy if the device itself employs strong security measures, but the biometric system may be less accurate given limitations associated with on-device computing resources.

misuse or harms. It could include, for example, guardrails that can be put in place for downstream use, such as contractual terms prohibiting certain uses of data or models by third parties and by requiring certain data security measures to be in place.

However, OSTP should also recognize that biometric technology is still an emerging field and relevant benchmarks and best practices will continue to evolve. OSTP should allow for continuing innovation in this space. A US framework should encourage global interoperability and align with national and international standards through organizations like the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO).

******

Google appreciates this opportunity to provide a response to OSTP's request for information and looks forward to continued discussion on these important issues.