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.
Introduction - FaceTec, Inc. (a Delaware Corp.) is the leading global provider of 3D Liveness and 3D Face Matching software for remote identity verification platforms. FaceTec’s technology is currently used by U.S. federal and state governments, numerous foreign/sovereign governments, as well as hundreds of commercial entities to verify, enroll and reverify (authenticate) citizens, customers, and users. Examples include the Colorado Mobile Driver License, the Utah Mobile Drivers License, the U.S. Department of Homeland Security Mobile Trusted Traveler-related programs, the Canadian Parliament Remote Voting Verification System, and the United Arab Emirates Digital Dubai project.

Over 350,000,000 people on six continents have proven their Liveness remotely with FaceTec on smartphones, tablets, and webcams (including low-end & low-res devices), and with no observable age, gender, or skin tone bias. In 2022, FaceTec will enable well over 500,000,000 distinct 3D liveness checks globally.

To ensure real-world security, FaceTec operates the world’s first-and-only persistent $100,000 Spoof Bounty Program, incentivizing hackers to attempt to beat its biometric security platform. It has successfully defended against over 105,000 bounty program attacks over the last 25 months, providing unmatched insight into the methods required to rebuff the most sophisticated threats to remote access management, identity proofing, and biometric verification systems.

We are proud to contribute a response. The White House Office of Science & Technology Policy RFI asked six broad questions. FaceTec’s answers follow, with the questions the information pertains to listed in the header of each section.

Thank you.
1) Biometric Overview (Questions #1, #2, #5)

Biometrics is the measurement of data, usually digital, that was collected from unique personal physical attributes and can be compared to other like-kind biometric data. There are many biometric modalities, including fingerprints, face images, iris images, retina images, blood vessels images, voice recording, signature, behavioral, and DNA, among others. Biometric data can be used in several ways but is typically used in one of two ways, personal Identification, and legal identity Verification. Any biometric data can potentially be used for identification but only some biometric data can be used to verify a person’s legal identity, and even fewer are effective at verifying a person’s legal identity remotely. Moreover, biometric systems are designed for the collection of the biometric data, which to the subject, may be Voluntary or Involuntary. The differences are not well understood by the public or media, and that is why education about this topic is critical to making informed policy decisions.

Identification is the process of connecting known data to unknown data from an individual, so that the identity of the subject can be known, or at least estimated with a probability. Identification answers the question “who is this person?”. Identification functions compare the yet unknown biometric against a dataset of existing or known biometric data that has been bound to identity details, like name, for example. The software determines if a match or even multiple matches exist to any known identities at the given match confidence level. The process is often called a “one-to-many” match, or 1:N, and data collection for it can be voluntary or involuntary. There are many applications of 1:N matching. Law enforcement agencies “identify” involuntary suspects by comparing the suspect’s fingerprints to databases of existing known criminal prints. Today, some government and commercial organizations collect biometric data (usually face images or video frames) from subjects, without permission, to be compared against criminal databases, simply to determine if there is a possibility that a criminal is present. Many believe this application raises privacy concerns. Conversely, employers screen voluntarily collected biometric data from job applicants using a similar software method to uncover potential criminal history during the job application process. In this case, the applicant volunteers to be compared to others in the database, eliminating privacy concerns. Additionally, stakeholders, like banks and e-commerce vendors, use identification and one-to-many matching to mitigate
identity theft-related frauds. Therefore, ethical ramifications of biometric systems hinge largely on the specific application and the voluntary or involuntary nature of the subject person’s enrollment.

**Verification** is the comparison, for the purpose of confirmation, of two pieces of data that are presumed to be known. The stored, trusted biometric data of a vetted individual that has been bound to a legal identity, and the live biometric of a person claiming to be that individual. Verification answers the question for the relying party, “Are you who you say you are?” Verification is normally a voluntary action and is often referred to as a “one-to-one” match. Biometric verification is utilized in access control systems, like attempting to log in online after the enrollee’s identity is established. Biometric Verification is becoming pervasive in remote and unsupervised networks, like the internet. The COVID pandemic highlighted the importance of remote user verification, as identity theft and online fraud exploded. The marketplace for verification applications that run on devices the general public already owns, is huge. When devices like PCs, laptops, and smartphones can be used as legal identity verifiers, identity theft and online fraud can be stopped almost completely.

2) **Biometric Viability** (Questions #1, #2)

Any biometric data can be used for either identification or verification. Fingerprints, handwriting, and DNA have long been used in law enforcement, because of their latency potential. Additionally, very many large government databases exist, containing face images. Police mugshots, driver license photos, passport photos, national ID card photos, and other credentialing applications are ubiquitous and rely on face image data almost exclusively. To follow, extensive academic research on fingerprint and face biometrics exists. The U.S. National Institute of Standards & Technology (NIST), along with many other research entities, have researched fingerprint and face biometrics for decades. Moreover, human beings have evolved to communicate by seeing, talking, and listening. Thus, the natural human interface, to computer systems, follows natural human evolution, including face and voice.

The existence of such infrastructure has several implications. First, there is a limited business case supporting the development of biometric modalities, beyond
face, voice, fingerprint, DNA, and signature. Second, substantial academic research exists for these established modalities, while limited research data exists for alternative biometric technologies. Given all this, it’s likely that fingerprints, signatures, DNA, and face biometrics will remain the standard biometrics in law enforcement and forensic investigation, while face and voice biometrics will remain the standard modalities for commercial and civilian applications.

3) Probabilistic Biometric Match Outcomes (Questions #2, #4)

Biometrics can make two basic errors: False Match (FM), also known as False Accept, and False Non-match (FNM), also known as False Reject. False Accepts occur when the system mistakenly matches biometric data from different people. False Reject occurs when the system fails to make an appropriate match to the person who did provide both biometric data samples. A False Accept error could identify someone as someone they are not, setting the stage for a wrongful conviction or granting unauthorized access. A False Reject could fail to identify or verify someone, setting the stage to erroneously deny authorized access to privileges. Any of these errors could result in potentially catastrophic outcomes for individuals and society. Importantly, vendors with inferior technologies often tweak or skew their technology to minimize either False Accept or False Reject to artificially generate more impressive results in certain tests. Therefore, a better measure of a biometrics performance capability describes both False Accept and False Reject, relative to one another. Further, recent breakthroughs in face biometrics have substantially raised its potential utility beyond any other.

No biometric can ever be 100% accurate, because it is a derivative of the original biological human. Therefore, biometric matching relies on statistical probabilities. Biometric match results are probabilistic. To follow, increasing the amount of data, measured in a biometric match, increases the potential match accuracy and confidence. Regarding face liveness and biometric matching, there are two-dimensional systems (2D) and three-dimensional systems (3D). While 2D matching systems measure data from X, Y coordinates only, gathered from the 2D face image, 3D systems capture orders of magnitude more data, by measuring data from X, Y, and Z coordinates, as well as the 4th dimension, time, in some cases. Thus, 3D systems provide inherently and substantially higher potential Liveness and match confidence than any 2D system. This is why Apple adopted 3D for its
FaceID face authentication technology for the iPhone. Moreover, 2D face systems are subject to distortions in the image data that can confuse the matching algorithms and result in False Accepts, False Reject, and bias towards skin tone, age, and gender. Face distortions in 2D photos limit the potential biometric match confidence of 2D face matching systems. However, 3D face liveness and matching systems are not negatively impacted by perspective distortion, raising their match confidence levels far beyond 2D capabilities. FaceTec reports a false accept error rate of 1 per 12.8 million attempts, with a 1% false reject rate, orders of magnitude more confidence than 2D systems, and even more accurate 3D face matching algorithms are coming in 2022.

4) **AI, Machine Learning and Bias** (Question #4)

While biometrics have been researched and utilized for decades, AI used in conjunction with biometrics is relatively new. With that, the industry has observed some bias in AI-driven biometrics that can be corrected by ensuring correct system design and utilizing improved face biometric technologies.

There may be numerous sources of bias, but today, there are two largely recognized sources of such bias. The first regards AI itself and the training sets that are used to enable machines to “learn”. If the training sets are not sufficiently diverse, the AI will effectively learn to favor the perspective color of the training set. Thus, to advance inclusivity and mitigate skin color, gender, and age-based bias, the training set must be sufficiently diverse.

Second, 2D systems routinely gradient levels of light reflection, refraction, and contrast. Importantly, darkness is not a color, but the absence of light of any wavelength. Darker skin is darker because it absorbs more visible light wavelengths, rather than reflecting them to the sensor. So, 2D systems that rely on light reflection receive less data as the skin tone darkens. Thus, as quantities of light data fall with darker skin the potential for match accuracy is diminished. Similar biases can occur when a subject is wearing makeup, and with young children who have fewer unique characteristics on the skin, and thus any 2D system’s potential accuracy and confidence is less than a well-executed 3D system because with 2D there is simply fewer data to measure for all users, but that will negatively affect some users more than others.
Conversely, 3D face liveness and biometric matching systems do not rely exclusively on gradient levels of light reflection, refraction, and contrast. Rather, 3D systems rely on the actual physical shapes of the face and related attributes. Thus, 3D does not present measurable bias, regarding skin tone, gender, and age.

5) Liveness, Spoofing, Honeypots, and Spoof Bounty (Questions #2, #3)

Liveness detection is a process to determine if a computer is interfacing with a live human, in real-time, and is most valuable in remote and unsupervised identity verifications. Liveness determines if it is a real, living person, while biometric matching determines if it is the correct, real person. Liveness detection mitigates many forms of presentation attacks, including photo presentations, deepfake videos, or mask replica presentations. Additionally, liveness must mitigate “camera bypass attacks”, where hackers attempt to bypass biometric systems completely by injecting video images into the system that replace the legitimate images that would have been captured by the camera. Biometric spoofing and bypass attacks have become very sophisticated, as these examples demonstrate, https://liveness.com/#VendorsSpoofed.

Without robust liveness detection, biometric matching would be increasingly vulnerable to these remote fraud attacks. Therefore, biometric liveness detection should be considered a required, and primary, first line of defense to mitigate identity-related attacks.

There are various types of biometric liveness defense:

- **Active Liveness** commands the user to successfully perform a movement or action like blinking, smiling, tilting the head, and track-following a bouncing image on the device screen. Importantly, instructions must be randomized and the sensor/system must observe the user perform the required action. Active Liveness methods can stop unsophisticated fraudsters, but they will not stop knowledgeable hackers without many additional layers of security, that most active Liveness vendors do not possess.

- **Passive Liveness** relies on involuntary human traits like eye saccades, pupil dilation, skin texture, hair texture, reducing user friction, and session abandonment. Passive liveness only asks the user to “be themselves” and
thus, what a fraudster must do to successfully attack the system is more difficult to ascertain. This forces attackers to guess about what attack vector to use. When Passive Liveness is paired with 3D face data and camera feed security assurance it can determine if the biometric data is first-generation captured just moments before the analysis takes place, and not a presentation attack or injection of data that was previously collected. Significantly higher security levels can be achieved when the face images are captured securely with a verified camera feed, and the image data is verified to be captured in real-time by a device Software Development Kit (SDK). Under these circumstances, both liveness and match confidence can be determined concurrently from the same data, mitigating many potential vulnerabilities.

- **Multimodal Liveness** utilizes numerous liveness modalities. This often requires the user to “jump through hoops” of numerous active liveness tests and increases friction and session abandonment.
- **Liveness & Three-Dimensionality.** A human must be 3D to be alive, while a mask-style artifact may be 3D without being alive. Thus, while 3D face depth measurements alone do not prove the subject is a live human, determining that a spoof artifact two-dimensionality proves the subject is not alive. Regardless of camera resolution or specialist hardware, three-dimensionality provides substantially more usable and consistent liveness data than 2D, dramatically increasing accuracy, highlighting the importance of 3D depth detection as a component of stronger liveness detection.

More information on biometric spoofing and liveness is available at [Liveness.com](http://Liveness.com).

Today, there is much debate about the security implications of using biometrics. Some observers describe potentially catastrophic implications of moving biometric data from one device to a database and storing such data in a centralized database. A biometric honeypot is a concept describing the possibility that a centralized biometric database could be breached and its contents stolen. This could potentially compromise the victims' identities from that point forward. These fears can be mitigated relatively easily by utilizing properly designed cryptographic security systems. More effectively, however, if that biometric data was stored in an altered format, such that it could not be used to steal an identity, the hacker's motivation to breach the database and steal the biometric data disappears.
An identity verification system should be designed to accept only concurrently captured liveness and matching data within the same data flow. After liveness is confirmed, liveness data should be deleted. With that, the remaining matching data, lacking the required liveness data, would be rejected by the identity verification system upon resubmission. This would render the remaining biometric data unusable by a hacker, mitigating or even eliminating honeypot risk.

Conversely, designing identity management solutions to minimize the use, or even avoid biometric data creates significant vulnerabilities that have enabled some of the most notorious data breaches, including the Solarwinds breach. That vulnerability is known as “The PKI Fallacy”. More about the PKI Fallacy is found here: https://youtu.be/Cp8EvCduvLU.

Industry standards, like those developed by the International Organization for Standardization (ISO) and The National Institute of Standards and Technology (NIST), might not address the most current types of spoof attacks. This is because, while hackers and cyberattack vectors evolve in real-time, utilizing the most current available technologies and techniques, technology standards must remain fixed for long periods. ISO standards, for example, once ratified, cannot be changed for five years. Thus, an ISO standard for Biometric Liveness, Presentation Attack Defense (PAD), and anti-spoofing capabilities could be several years old and remain mandated by various stakeholders. Moreover, certification laboratories, like iBeta, are frequently bound to certify vendor compliance and conformity to PAD-related standards that are not capable of defending against the most current spoof attack vectors, like deepfake puppets and bypass attacks. Despite this, many vendors today market such certification as evidence of their ability to defend against the most modern attack vectors. It is likely their customers, which may include government agencies, do not know their defenses are incapable of defending against attacks beyond an outdated standard.

Consequently, FaceTec has developed a $100,000 Spoof Bounty Program (www.spoofbounty.com) that invites hackers to attempt to penetrate the FaceTec 3D Face Liveness software. To date, FaceTec has defended against over 105,000 attacks over the last 25 months. FaceTec systems were spoofed only two times, allowing FaceTec to close those vulnerabilities while providing FaceTec with invaluable data to understand the most current spoof attacks. Consequently,
FaceTec routinely consults with and educates government and large enterprise stakeholders around the globe.

6) **Government Trust Anchor** (Questions #3, #5)

*“You are who the government says you are”.* Birth certificates, social security cards (numbers), driver licenses, passports, Medicare and Medicaid cards, national IDs, among others, are government-sponsored, identity-related documents that we use to proclaim who we are in society. With that, government-sponsored identities represent the “anchor of trust” for society’s identity verification needs. It makes sense that the government represents the best source of information to be used in identity management schemes, and is best suited to “vouch” for citizen identities.

Devices are not humans and humans are not devices. By binding a privilege credential to a device, without binding the credential to the appropriate identity, any identity management system is easily compromised. This is exactly the vulnerability that led to the SolarWinds breach. The vast majority of today’s data breaches and online frauds exploit weak user authentication, associated with strong device authentication. Without strong, liveness-proven biometric user authentication, the strong credential/device authentication enables Advanced Persistent Threats (APTs), like SolarWinds.

By matching a liveness-proven biometric with the government-managed citizen identity profile (e.g., DMV or Dept of State database), that same biometric would be the ideal identity verifier for citizen and consumer identity-related needs. Taking a selfie can provide all the necessary liveness and biometric matching data necessary to instantly verify one’s identity in society and marketplaces. All biometric data would reside behind the government firewall, yet be rendered unusable for resubmission, avoiding honeypot risk. A government identity verification submission would be compared to the biometric, bound to the civilian identity, and associated with a driver’s license number or social security number. An API system would generate a binary “Yes” or “No”, response. The relying party would receive the API response and accordingly approve or disapprove the transaction. The establishment and maintenance of such a root identity require secure remote human verification and authentication technology that did not exist until recently.

The FaceTec technical diagram informs subsequent business models for identity issuers around the world, follows:
Conclusion

Thank you for the opportunity to provide our insight into the current state of the market and art in biometrics, and proper citizen/user identity proofing, enrollment, and verification. More information can be found at www.facetec.com.