IBIA
International
Biometrics+Identity
Association

Office of Science and Technology Policy
The White House
1650 Pennsylvania Avenue, NW
Washington, DC 20502

January 14, 2022

Submitted Electronically via email to: BiometricRFI@ostp.eop.gov

Subject: OSTP Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies (*Federal Register* Document No. 2021-21975)

On behalf of the International Biometrics + Identity Association (IBIA) and its membership, we are pleased to submit this information to OSTP in response to the Request for Information (RFI) regarding "Public and Private Sector Uses of Biometric Technologies" (*Federal Register* Document Number 2021-21975).

Information Requested

Our responses provide an overview of the specific use of biometric technologies in the public and private sectors, as requested in RFI topics 1 through 6.

Topic 1: Descriptions of use of biometric information for recognition and inference.

Biometrics are unique physical (anatomical or physiological) or behavioral characteristics which can be used to identify individuals. Biometric technologies capture, process and measure these characteristics electronically and compare them against existing records to create a highly accurate identity management capability. As previously mentioned, common physical biometric indicators in use today include fingerprints, faces,[1] irises, voices, and DNA, among many other modalities.

Biometrics have been around for over 100 years in various forms around the world and for various use cases. In the U.S., the techniques of measuring fingerprints, latent fingerprints, and palm prints grew in popularity among the law enforcement community in the early 20th century. The modern digital version of biometrics in use today by law enforcement or national security professionals was developed about 45 years ago. The technology has progressed rapidly in the past 20 years, largely due to heavy investment in research and development. This progression has also accelerated in the last 10 years due to advancements in computing technology that made practical the deep neural networks associated with machine learning approaches to biometrics.

[1] For more information, *see* https://www.ibia.org/download/datasets/5733/IBIA%20Facial%20Recognition%20Use%20Cases%20FINAL.pdf.

Topic 2: Procedures for and results of data-driven and scientific validation of biometric technologies.

Such procedures largely fall into two categories: algorithm testing and full system testing. Our member companies do both types of testing, both by performing internal tests and by submitting their algorithms and systems to independent, third-party testing entities.

Most biometric algorithms (including those of our member companies) are subjected to the objective and public testing of the National Institute of Standards and Technology (NIST). NIST has been researching, testing, and developing standards for biometric technologies for six decades.[2] NIST testing, which uses known and repeatable data, has demonstrated that top-performing face recognition,[3] iris recognition,[4] and fingerprint[5] algorithms can achieve accuracy rates of over 99%. For face recognition technologies, NIST has specifically evaluated algorithm performance across age groups, racial groups, and sexes. Of particular note, NIST has found that the top-performing algorithms exhibit "undetectable" differences in false positive error rates across demographic groups based on race and sex.[6]

For most biometrics other than DNA, statistical results of testing are often graphically displayed in the form of Receiver-Operator Characteristic (ROC) or Detection Error Tradeoff (DET) curves. ROC curves show how an algorithm performs as its discrimination threshold is varied. That is, how the true positive rate of matching or identification (sometimes called "accuracy") varies as the acceptable false positive ("impostor") rate is increased. DET curves show how the false negative rate (truthful match rejected) varies as the false positive rate (impostor accepted) varies. Such curves help an operator set an algorithm threshold that is optimal and acceptable for their application, process, and risk tolerance. For a specific example of the application of such testing technique for face recognition, see the IBIA analysis of NIST testing of demographic differentials in IBIA member algorithms.[7]

Operational performance[8] of biometric technologies also depends on environmental conditions that vary across use cases and functional applications. The impact of such factors on overall biometric technology performance can be more objectively quantified in testing, such as Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Biometric

[2] https://www.nist.gov/programs-projects/biometrics

[3] https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing

[4] https://pages.nist.gov/IREX10/

[5] https://www.nist.gov/programs-projects/fingerprint-vendor-technology-evaluation-fpvte

[6] P. 8 – https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

[7]https://www.ibia.org/download/datasets/5725/IBIA%20Diversity%20Data%20Analysis%20Unabridged%20FINAL.pdf

[8] Assessing operational performance often entails evaluating not only accuracy but also factors including capture rate, failures to enroll, and speed of operation.

Rally tests, which measure biometric technologies' full system performance.[9] These Biometric Technology Rallies, which DHS S&T typically holds at the Maryland Test Facility (MdTF), include diverse test subjects and environmental factors that are present in a variety of operational settings, including TSA and CBP security checkpoints in airports. Even in these environments, DHS S&T Biometric Rally tests have demonstrated biometric technologies' high accuracy rates. Of particular note, recent face recognition technology Rally tests have demonstrated that top-performing face recognition technologies are over 98% accurate at identifying individuals wearing face masks and are over 99% accurate at identifying individuals who are not wearing face masks.[10]

For DNA use in human identification, a number (currently 20 for FBI CODIS) of genomic loci with so-called short tandem repeat sequences, or STRs, is used for comparing DNA samples. The probability of match for two DNA samples at each locus can vary by population sub-group, so population statistics ("popstats") are used to qualify the probability of match. These popstats are derived from genetic population models developed over the years. In practice, a DNA match is further qualified by the number of loci detectable in the sample vs the reference DNA profile. Like other biometric modalities, the data and science behind DNA uses for human identification are well-developed.[11]

Topic 3: Security considerations associated with a particular biometric technology.

Generally, the use of biometric factors in identity management increases the security of the systems that use such factors in both logical and physical security applications. In logical security applications, we cite NIST FIPS-201 section 6.3.2 where it states that the addition of a biometric for logical access control imparts "HIGH" or "VERY HIGH confidence."[12] The use of such techniques can prevent breaches due to threats from insiders sharing or using credentials from others to gain access to more compartmentalized data to which they aren't entitled. While this is true and effective for preventing access intrusions "through the front door", cyber threats due to network intrusions or unwitting user installations of malware can present a much more serious challenge. There is no biometric panacea for prevention of cyber-intrusions, and there is no substitute for diligent cyber hygiene, effective cyber policies, and effective automated cyber intrusion tools. Multi-factor authentication using biometrics is one layer in what needs to be a multi-layered cybersecurity defense.

Much has been made of so-called "presentation attacks" using fake or spoofed biometrics. Defense against this type of attack is why FIPS-201 insists on in-person biometric enrollment, so the operator can verify that the biometric(s) presented by the subject at enrollment is (are) indeed genuine and not fake. Subsequent detection of impostors using a valid enrolled subject's biometrics (e.g. fake fingerprint, print-out of a face, contact lens covering iris) are either detected by in-person witness, or automated sensor actions such as liveness detection. Methods of

[9] https://www.dhs.gov/science-and-technology/biometric-technology-rally

[10] https://mdtf.org/Downloads/MatchingSystemResults.pdf

[11] https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet

[12] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf

liveness detection vary by biometric modality. For example, to mitigate the printed face attack, the sensor must detect eye blinks or eye motion or changes in facial expression or aspect. Newer iPhones image the face in 3 dimensions, which effectively counters the 2-dimensional printed face attack. For fingerprints, the sensor may do liveness detection by sensing galvanic skin response, skin spectral response, or subcutaneous blood flow. Painted contact lenses as an iris spoofing approach are detected in infrared imaging, and even more advanced iris spoofing detection techniques are being developed.[13] Replay attacks (recording someone's voice and replaying it to spoof speaker verification) can be detected both through spectral (frequency) analysis as well as by prompting the speaker to speak voice segments that could not have been recorded earlier (as well as adding other identification factors like a PIN or texted security code – leveraging the power of multi-factor authentication).

For physical security, we cite the example of CBP's use of facial biometrics for matching to passports.[14] "This enhanced process using facial biometrics only takes a few seconds and is more than 98 percent accurate." As noted in the IBIA paper cited previously, the 98% accuracy cited by CBP is far superior to the typical human trying to do facial matching or recognition. "To date, more than 119 million travelers have participated in the biometric facial comparison process at air, land, and seaports of entry. Since September 2018, CBP has leveraged facial biometrics to prevent more than 1,100 impostors using genuine travel documents from illegally entering the United States at air and land ports of entry."

Topic 4: Exhibited and potential harms of a particular biometric technology.

Answers to this question could fall across two different categories, depending on the interpretation of the question. One category is potential harms of the technology itself, and the other is harm that could occur from the applications of the technology.

To the first category, we are not aware of any exhibited or potential harms of the biometric technology by itself. The infrared illumination required by iris recognition is harmless. The use of contact-style fingerprint readers in high-volume public applications is sometimes cited as a potential source of contagion, but that hasn't proven to be the case for SARS-CoV-2, which is transmitted via inhaled microdroplets. Some contact fingerprint readers have UV sanitizing illumination that turns on between uses of the readers, thus sanitizing them. In other cases, the operators simply swab the capture platen with alcohol between uses, which both sanitizes and cleans the surface for better capture of the next fingerprints.

For the second category, as with any technology, people can misuse it. To counter this, the IBIA has developed ethical principles and best practices, detailed in our responses to Topic 6 sub-paragraphs. In short, we don't support uses of biometrics to oppress a country's citizens or to discriminate against any class of people or suppress First Amendment rights to free speech and assembly. We don't support real-time uses of biometrics for surveillance (e.g. in conjunction

[13] https://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=5&f=G&l=50&co1=AND&d=PTXT&s1=9,934,436&OS=9,934,436&RS=9,934,436

[14] https://www.cbp.gov/newsroom/local-media-release/cbp-expands-simplified-arrival-four-ports-entry-washington-state

with video surveillance) unless authorized by court order, similar to wiretap restrictions. However, forensic biometric analysis after crimes have been committed should always be allowed, as in the case of the Capitol insurrection or the Boston Marathon bombing. Proposals to ban the technology mean that urgent uses of the technology for forensics after emergent events may not be possible.

To be clear, identity verification such as performed by TSA or CBP in the course of their legal obligations is **not** surveillance (see Topic 6f). Use of biometrics by companies for such things as security, convenience and attendance recording should always be allowed, so emerging state restrictions (such as BIPA[15] in Illinois) are inappropriate and should be preempted by Federal law.

Topic 5: Exhibited and potential benefits of a particular biometric technology.

One of the most striking use cases that illustrates the benefits of biometrics is in the case of travel under pandemic conditions. For example, the TSA has developed self-service credential verification stations ahead of checkpoints, which allow passengers to insert their own ID into a machine and have their face (unmasked at that point) matched to the image. TSA has also piloted face matching without the credential, leveraging capabilities first demonstrated and now widely deployed by CBP. The system developed by CBP is called "Simplified Arrival", and some people characterize it as "your face is your passport". [16] In both the TSA and CBP cases, travelers can verify their identities without having to interact closely with officers, thereby saving time, increasing accuracy, and maximizing hygiene. If you've ever been on a cruise ship, you know how much time it takes to embark and debark the ship, particularly if customs and immigration processing is required. Face recognition simplifies and speeds the process. Based on feedback from participating cruise lines, CBP reports a reduction of debarkation times as much as 30%, with a concomitant improvement in passenger satisfaction survey scores vs. non-biometric debarkation processing.

Generally, travelers appreciate touchless processing, and biometric sensors are available for touchless processing using face recognition, iris recognition, fingerprint recognition, voice recognition, and gesture recognition. Other environments where touchless biometrics are beneficial include chemical or biological hazard areas, nuclear or explosive materials processing, and applications that require hands-free for other purposes.

The benefits of fingerprints, latent prints, and DNA are well-known for forensic purposes, and consumers are increasingly willing to use fingerprint or face recognition technologies to unlock their smart phones and other devices. Voice processing, or more specifically voice verification, has been used for some years in verifying the voices of callers for financial transactions or remotely providing government services.[17] Behavior biometrics are used for continuous authentication of computer system users, and to detect insider threats based on indicative

[15] https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

[16] https://www.cbp.gov/sites/default/files/assets/documents/2018-Aug/Simplified_Arrival_Fact_Sheet.pdf

[17] https://www.ato.gov.au/general/online-services/voice-authentication/

changes in behaviors. Face and image recognition technologies have also helped officers generate investigative leads for crimes including bombings, insurrections, as well as human and child trafficking.

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

IBIA has published a number of documents outlining our views on governance programs and best practices that help mitigate risks and support the benefits that biometric technologies can produce. A significant example of this is our "Ethical Use of Biometric Technology"[18] white paper, which we believe is foundational for our industry.

Topic 6a: Stakeholder engagement practices for system 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.

There are numerous and diverse applications of biometric technologies, and more will emerge over time. For that reason, it must be left to the use of a specific application to evaluate how to appropriately apply these general principles, taking into consideration the: a) application; b) purpose of the application; c) risks and consequences of abuse; d) personal and non-biometric data used; and e) legal and regulatory constraints, including privacy laws. There are no less than 29 federal laws that include privacy provisions, and diverse and proliferating laws being proposed and enacted at the state level.

Given the complexity and diversity of both the technology and the legal/ethical considerations, IBIA focuses on education and outreach to encourage enlightenment and diversity of dialogues on these important topics. To this end, IBIA and its members have participated and, in many cases, led the efforts to engage stakeholders and advocate for guidelines regarding policies, laws, principles and best practices. Examples include:

- **NTIA General Framework for Privacy** - IBIA Participated in the Department of Commerce, National Telecommunications and Information Administration (NTIA), Multi-Stakeholder Process to develop and publish a general framework for the commercial use of facial recognition titled the "Privacy Best Practice Recommendations for Commercial Facial Recognition Use."[19]
- **Annual connect:ID / Identity Week Conference** – IBIA co-sponsors this annual event that brings together government, academia, industry, privacy and policy experts all for the express purpose of discussing not only the latest trends in the technology, but also best ways to test, deploy, and enhance the technology in support of our customers and their missions. We also host specific panels on the ethical use of automated identity data as a social good.[20]

[18] https://www.ibia.org/download/datasets/5741/IBIA%20Ethical%20Use%20of%20Biometric%20Technology%20FINAL.pdf

[19] https://www.ntia.doc.gov/other-publication/2016/privacy-multistakeholder-process-facial-recognition-technology

[20] https://www.terrapinn.com/exhibition/identity-week-america/index.stm

- **Active Member of the Future of Privacy Forum** – IBIA has been an active member of the Future of Privacy Forum for 5 years. We have had a strong, collaborative relationship. Together, we have worked with FPF to co-develop papers on privacy issues, biometrics and identity technology, and education efforts.[21]
- **Publication of White Papers and Industry Best Practices Guidance** - IBIA routinely publishes white papers on privacy policy principles, ethical use, impact of demographics, security and safeguarding data, industry best practices, and implementation guidance for use cases of biometric and identity technologies. [22]
- **Participation in Public Discourse and Debate** – We have testified before various Congressional Committees on various topics relating to biometric technologies over the past 10 years.[23] [24]

Topic 6b: Best practices or insights regarding the design and execution of pilots or trials to inform further policy developments.

We are not aware of published best practices in this area, though the industry and most users follow some generally accepted principles which may vary depending on the use case and biometric modality (or modalities) employed. For example, for a biometrically enabled travel lane (ship debarcation, airport immigration, security checkpoint, jetway boarding), the trial or pilot should be limited in scope, with alternative travel lanes (e.g. "opt-out"), well-advertised, and attended by observers and helpers who can note difficulties and assist travelers who encounter trouble moving through the trial lane. "Well-advertised" can be local signage, instructional videos on display screens, recorded announcements, and public notice (e.g. websites and social media) all the way to formal notices of proposed rulemaking (NPRM) in the Federal Register. Comments from the public on the pilot both before (e.g. in response to a solicitation of comments on an NPRM) and after experiencing the pilot (e.g. satisfaction surveys) inform the results of the trial and help the organizers make improvements and respond to needs and feedback. This valuable feedback can be utilized in associated policy development.

Topic 6c: Practices regarding data collection (including disclosure and consent), review, management (including data security and sharing), storage (including timeframes for holding data), and monitoring practices.

See our response to topic 6h. Both our commercial best practices and Government PIAs and SORNs address these topics.

Topic 6d: Safeguards or limitations regarding approved use (including policy and technical safeguards), and mechanisms for preventing unapproved use.

[21] https://fpf.org/

[22] https://www.ibia.org/resources/white-papers

[23] https://science.house.gov/hearings/the-current-and-future-applications-of-biometric-technologies

[24] https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=105757

While biometrics are not secret, most agencies and companies treat them as personally identifiable information (PII), especially in conjunction with associated biographics. Therefore, the best practice is to protect such data by encryption at rest and encryption in transport. Access to the data is protected by mandatory (e.g. classification level) and discretionary (e.g. need to know) access control (often both logical and physical), usually enforced by required multi-factor authentication as referenced in Topic 3. Security logs record who has accessed the data, for what purpose and when, and periodic audits verify that the logs have recorded activity that is permitted (or not). Automation is available to monitor the logs for suspicious activity so that immediate alerts are generated between audit periods. This approach mitigates the insider threat (an authorized user who abuses the system). Operationally, automated workflow systems can ensure multiple levels of review are conducted in accordance with policy (e.g., automated biometric system finds candidates, which go to an examiner to refine, which go to a supervisor for review and approval or rejection).

Topic 6e: Performance auditing and post deployment impact assessment (including benefits relative to current benchmarks and harms).

See our response to topic 6h. IBIA advocates best practices to include post-deployment audits of operations to ensure that proper procedures are being followed, that the system operates as intended, and there is no abuse or insider threat. We do recommend that operators periodically review current performance testing on biometric systems (e.g., through recent NIST testing publications) and consider upgrades where advancements show pronounced benefits (e.g. security, accuracy, throughput, response times, cost) over legacy systems.

Topic 6f: Practices regarding the use of biometric technologies in conjunction with other surveillance technologies (e.g., via record linkage).

This question implies that the author considers biometric technologies to be surveillance technologies, and this is not the case. Surveillance is using humans or automation to persistently observe an environment to derive intelligence, detect adverse behavior, or – when recorded – to forensically analyze circumstances leading up to an event of interest (perhaps for purposes of attribution). There are many forms of surveillance, including aerial imagery, data mining, social network analysis, computer, communications, RF (including RFID and geolocation), geophysical, audio (e.g. gunshot detection and location) and video surveillance. The most common form of surveillance in civilian use today – video monitoring of roads and cities – is very useful for traffic flow monitoring, security monitoring, and emergency dispatch awareness – but this infrastructure will also be foundational to some functions of smart city evolution. However, city surveillance with real-time facial recognition should be governed by policy and law and used in limited (perhaps only court-prescribed) circumstances. We tend to think of these types of applications for identifying criminals or terrorists, but there are other applications of the technology, like finding missing children, identifying exploited children, and identifying trafficked, missing or disoriented adults (e.g., with amnesia, dementia or Alzheimer's disease). Facial recognition is always warranted for forensic analysis after an emergency event, especially when no other useful evidence is immediately found, and the need is urgent.

A facial recognition system is designed to present matching candidates from its accessible gallery(s) of faces to that of the subject of interest. Contrary to popular belief (or urban legend), there is no single comprehensive government database of faces of US citizens, nor is there any unified national surveillance system. If the facial recognition gallery(s) do not have a face already enrolled, the system cannot match or identify the subject of interest.

As for record linkage, linking a person's biometric (face) to other information, while possible, is less useful to a (cyber) criminal than linking a Social Security number to a birthdate. The latter can be used to steal a person's identity, while a face or fingerprint by itself cannot. Indeed biometrics, when available, can expose such subterfuge, as in the 1,100 cases cited previously where CBP has discovered people attempting to enter the country with fraudulent or stolen passports.

Topic 6g: Practices or precedents for the admissibility in court of biometric information generated or augmented by AI systems.

Biometrics (e.g. fingerprints, DNA) have been admissible in court for years (albeit usually with a human examiner to provide testimony). Presumably, this question refers to face recognition, not by eyewitness, but by machine (algorithmic) search. There is precedent for admissibility of "predictive coding" in court.[25] However, as the technology is rapidly evolving, it is reasonable to expect that legal precedent will evolve as well. The issues of explain-ability, fairness, and trustworthiness apply here, and this is an active topic of development for many applications of machine learning (sometimes known as AI/ML).[26] Meanwhile, the FBI and others are treating machine-generated candidates in facial searches only as investigatory leads, especially where there is a paucity of other leads. That is, it isn't actionable evidence, and certainly not evidence of guilt. Other more traditional evidence must be discovered to confirm (or negate) such leads before more serious law enforcement actions are taken. We believe that this "human in the loop" operation is likely to remain the standard for the foreseeable future, and the process must be backed up by policy, training, oversight, access control, and periodic audit.

Topic 6h: Practices for public transparency regarding: Use (including notice of use), impacts, and opportunities for contestation and for redress, as appropriate.

For Government applications of biometrics, transparency is assured through the required publication of Privacy Impact Assessments[27] [28], and System of Records Notices.[29] [30] PIAs, for example, contain information on a system that includes a description, the information in the system, sources of information, threats to privacy, purpose and use of the system, why the

[25] https://scholar.google.com/scholar_case?case=6856971937505165396&q=da+silva+moore+v.+publicis&hl=en&scisbd=2&as_sdt=2,44&as_ylo=2012

[26] https://www.leidos.com/enabling-technologies/artificial-intelligence-machine-learning

[27] https://www.dhs.gov/publications-library/collections/privacy-impact-assessments-%28pia%29

[28] https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments

[29] https://www.dhs.gov/system-records-notices-sorns

[30] https://www.justice.gov/opcl/doj-systems-records

information is being used, legal authorities for operation, how long the information will be retained, with whom it will be shared, requirements for notice, consent and redress, security controls, and applicability of the Privacy Act. Regarding SORNs, from the DHS citation, "a system of records is a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual. The Privacy Act requires each agency to publish notice of its systems of records in the *Federal Register*."

For commercial uses of biometrics, IBIA has developed "Privacy Policy Principles" that provide general guidelines use of biometric technologies and data, while allowing implementers and operators to customize their approaches based on the biometric technology application(s) used and the potential risks and benefits associated with the given use-case.[31] In these Principles, IBIA recommends that implementers and operators of commercial biometric technology develop and publish privacy policies incorporating a Collection Limitation Principle, a Purpose Specification Principle, a Data Quality Principle, a User Limitation Principle, a Security Safeguard Principle, an Openness Principle, and an Accountability Principle. Others have developed similar frameworks and principles. A useful reference for law enforcement uses of face recognition technology is the Bureau of Justice Assistance Face Recognition Policy Development Template[32].

Conclusion

Thank you for giving us this opportunity to present this submittal to you and your colleagues at OSTP. IBIA is dedicated to the ethical use of biometrics and welcomes opportunities to participate in multi-stakeholder dialogues and to serve as a resource to policymakers and media outlets interested in discussing and working to address these important topics. We look forward to continuing the dialogue and working with your Office and other organizations and individuals who have also provided comments and insight for this RFI.

For More Information, Please Contact:

Robert A. Tappan
Managing Director
International Biometrics + Identity Association
1325 G Street, NW
Fifth Floor
Washington, DC 20005
Tel: (202) 888-0456;
e-mail: robert@ibia.org

[31] https://www.ibia.org/download/datasets/5717/IBIA%20Privacy%20Policy%20Principles%20FINAL.pdf

[32] https://bja.ojp.gov/sites/g/files/xyckuh186/files/Publications/Face-Recognition-Policy-Development-Template-508-compliant.pdf