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.
January 14, 2022

VIA ELECTRONIC SUBMISSION: [Redacted]

The Office of Science and Technology Policy (OSTP)
Eisenhower Executive Office Building
725 17th Street, NW
Washington, D.C., U.S.

Re: Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies (Document Citation: 86 FR 56300)

Introduction
The International Association of Chiefs of Police (IACP) is the world’s largest and most influential professional organization for law enforcement leaders. With more than 31,000 members in 165 countries, the IACP is a recognized pacesetter in global policing, committed to advancing safer communities through thoughtful, progressive law enforcement leadership.

While all policing decisions are fundamentally made by humans, the law enforcement community often uses appropriate technologies to help identify potential investigative leads which would otherwise be overlooked or extremely expensive and time-consuming to find. Literally millions of crimes would go unsolved and their victims left without justice were it not for certain technological and scientific processes which the computer age continues to provide. Additionally, digital evidence is pervasive, voluminous and extremely complex. Protecting the innocent requires an exacting and robust application of technology.

This is especially important in the current law enforcement environment. There are many challenges facing police leaders, including difficulties maintaining and hiring a police force, increasing crime, pandemic pressures, and justice reform expectations. Therefore, law enforcement executives need to take advantage of new technologies wherever possible to help alleviate these new challenges. All while maintaining the agency’s legitimacy and trust in the communities they serve. New public safety endeavors must be thoughtfully considered. Any technology must bring significant benefits to our communities that greatly outweigh risks. Especially when applied and managed within a mature policy and quality control context.

Our response to the Office of Science and Technology Policy’s (OSTP) Request For Information (RFI) is therefore based on where law enforcement has been with biometric technologies, where it is today and what we can see in the near future, especially regarding the enhancements Artificial Intelligence (AI) adds to such processes to assist in policing our communities. As will be set forth in greater detail below, the IACP strongly believes that AI-assisted biometric technologies are providing, and will continue to provide, substantial contributions to public safety in a wide range of disciplines. Any efforts to limit or burden the deployment or use of these technologies should be carefully balanced against the harm that the technologies are preventing.
Over the past three decades, the technology industry has risen to the challenges of the policing community. Initially focused on the first wide-scale biometric identifier (fingerprint matching), the technologies have transformed the successful prosecution of crime based upon not only eyewitness testimony and/or suspect admissions but also scientific study and digital evidence. The development of fingerprinting changed policing so much that virtually all criminal identification and background/history checks require the use of fingerprint-based lookups utilizing automated technologies as the first and primary step. In more than five decades of wide scale usage, the justice community and the public have completely accepted the use of fingerprinting as a trusted and important clue in criminal investigations. Fingerprints are so mainstream they are used for everything from clearing volunteers to work with children to providing top secret clearances for access to the most important critical homeland security information.

However, it is important to understand that Biometrics and Artificial Intelligence have been separate concepts to the law enforcement community until the last decade. In our response, we do not specify the intrinsic value or problems with any specific technology, but instead address how law enforcement, and specifically the IACP, understands and values the merger of these technologies, plus how we need to strongly encourage police agencies worldwide to deploy them appropriately, fairly, and with full transparency so that the necessary pillars of community trust, citizen support, and public privacy are strongly maintained.

Law Enforcement History in Biometrics
The law enforcement community's interest in biometrics is primarily in the ability of the technology to automate and improve the quality of currently manual processes. By its nature, law enforcement routinely involves the observation and identification of persons, property, and objects. The growth in both the population and the number and sophistication of crimes has challenged the ability of law enforcement agencies to fulfill their basic charge with the limited human and technological resources they possess. Consequently, law enforcement has integrated advanced communications and computer technology to improve operations, from radio technology in the 1930s to centralized computerized criminal information databases in the 1960s and 1970s. Just as those technologies helped make law enforcement more effective, efficient, and responsive to the community, tools that make use of artificial intelligence will further enhance policing services.

An Example of Biometrics in Law Enforcement
A key example has been the rise of the use of fingerprints in law enforcement. Beginning in the late 19th and early 20th century, fingerprints were discovered to be effectively unique biometric identifiers.

Latent prints are fingerprints present at a crime scene but not easily captured or imaged. A latent fingerprint examiner handles capture and identification processes, including taking photos of fingerprints or utilizing different methods of latent fingerprint identification in the crime scene and identifying the fingerprints by running them against the automated fingerprint systems.

Besides their use in crime scene forensics, they also had a powerful use in the Criminal Identification (CI) activity of law enforcement. Knowing the identity of an individual involved in an incident is key to understanding the nature of a crime and the individual’s possible prior acts. Consequently, at the time a suspect is booked in jail, fingerprints are captured to determine the person's identity. This is
important if the subject has used other names (aliases) for previous arrests identification. Most importantly, the fingerprints are captured for the purposes of recording the arrest and/or conviction information in a permanent file associated with that person. Finally, captured fingerprints will typically be used to determine the person’s prior arrest and conviction record.

Initially local agencies and later the Federal Bureau of Investigation (FBI) began cataloging criminally involved fingerprints in America. By 1971, the FBI had over 200 million fingerprints on file. The quantity and size of this catalog demanded a technology solution to be able to take a subject’s fingerprints and be able to compare them to the full catalog that the FBI possessed. This has resulted in several generations of systems that were initially developed to handle fingerprint comparison. These systems, until recently, evolved without the use of today’s AI. The latest iteration is the FBI’s Next Generation Identification system. NGI handles not only fingerprints, but other biometrics, such as facial, retinal, and iris comparisons.

Operationally, these next generation systems have been able to handle the demands of growth. However, there are limitations. Unless a perfect set of data is presented, such as a quality fingerprint scan for a criminal history check, it is very likely a precise result of the search cannot be made. This results in either a low quality match or a candidate list of possible matches. At this point a certified fingerprint expert needs to become involved to evaluate the output of the biometric systems. To limit or remove any bias that may exist, blind identification - the confirmation of a latent print examiner's conclusion by another competent examiner who has no expectation or knowledge of the prior conclusion - is used.

The algorithm's limitations made a fundamental requirement for human intervention and review of any “match” before returning information to the requestor. This has become ingrained into the environment, such that even today on any potential match, the question arises “did a fingerprint examiner review and agree with the results?” Without that agreement by an uninvolved, certified examiner, there is no expectation the identification will hold up in Court.

Resulting Policy and Protections
Once fingerprint comparison became an accepted practice, there grew a need to create and maintain best practices based upon the latest technology, science, and accepted principles. Fingerprinting was the basis upon which the first forensic professional organization, the International Association for Identification (IAI), was formed in 1915. In 1977, this group developed the first professional certification program for forensic scientists, the Certified Latent Print Examiner program, which issued certificates to those meeting stringent criteria.

Human experts with these certifications provide a buffer and a control for the computerized biometrics systems. Furthermore, the experts provide legal accountability in situations where the results of a technology system may be in question. The IACP and law enforcement community understand that no technology is perfect, but the value of the technologies with human supervision is powerful and compelling.

No member of the public is ever charged with a crime based solely on the output of these fingerprint systems and processes. Instead the information produced is treated merely as a “lead” for the
investigative process. This concept, though different for each technology, is a fundamental guiding principle for the use of these technologies in law enforcement.

Lessons Learned from Automated Fingerprint Technology
There are several important lessons which are drawn from the law enforcement experience with fingerprints and helpful to guide use of other biometrics technologies and AI:

1. Automated Systems are Powerful – The growth of biometric identification both in subject identification and crime forensics has been possible because of the “automation” of the processes. When humans are the primary factor in the workflow, things become slow and error-prone.
2. System Limitations Must be Understood – The better the data, the better the results. When the data is limited or suspect - for example, in forensics - more human involvement is needed to ensure the quality and integrity of the system.
3. The Data Gallery Must be Protected – The gallery is the basis against which a present item is compared. This means the data, whether it is fingerprints or photos, must be of high quality and appropriate. Otherwise, the automation will fail with poor quality and less “narrowing” of possible matches.

There are other desirable outcomes from the adoption of biometric and fingerprint technology. Some individuals who were wrongly convicted using less technologically effective methods were released and convictions reversed. Furthermore, in these cases the actual perpetrator was identified for the first time through fingerprints. Without fingerprint technology, it is very likely these convictions would not have been overturned, with the wrong individual being incarcerated for a crime they did not commit. Similar positive outcomes have occurred with the development and deployment of DNA-based technologies. We expect that these new AI technologies will continue to find perpetrators that could not be identified with older technologies and processes. What is clear from our experience in law enforcement is that the best outcomes combine a human component, which ensures accountability, with the efficiencies gained through the use of automated systems.

Evolution of Artificial Intelligence
Artificial Intelligence (AI) is not a new concept. Scientists have been studying and conducting AI research in many forms since at least the 1940s. A recent report to Congress prepared by the Congressional Research Service noted that “the field” of AI research began in 1956, but an explosion of interest in AI began around 2010 due to the convergence of three enabling developments: (1) the availability of “big data” sources, (2) improvements to machine learning approaches, and (3) increases in computer processing power. This growth has advanced the state of Narrow AI, which refers to algorithms that address specific problem sets like game playing, image recognition, and navigation. All current AI systems fall into the Narrow AI category. The most prevalent approach to Narrow AI is machine learning, which involves statistical algorithms that replicate human cognitive tasks by deriving their own procedures through analysis of large training data sets. During the training process, the computer system creates its own statistical model to accomplish the specified task in situations it has not previously encountered. Experts generally agree that it will be many decades before the field advances to develop General AI, which refers to systems capable of human-level intelligence across a broad range of tasks.
Nevertheless, the growing power of Narrow AI algorithms has sparked a wave of commercial interest, with U.S. technology companies investing an estimated $20-$30 billion in 2016. Some studies estimate this amount will grow to as high as $126 billion by 2025. For purposes of this document, we are only concerned with Narrow AI.

**Use of AI in Law Enforcement**

This significant investment has brought forward new applications of AI to help law enforcement better utilize such things as Automated License Plate Recognition (ALPR) and Facial Recognition (FaceRec) technologies. It is important to realize that although much of law enforcement activities do focus on suppressing criminal activities, policing involves a broader array of services. For example, the police often interact with law-abiding citizens who may be at risk or in danger due to mental impairment or their status as a reported missing person. Experience shows many of the biometrics technologies have been useful for helping the police assist the public by being able to identify individuals in a non-intrusive way.

The lack of intrusiveness of biometrics also creates different challenges for law enforcement. Privacy advocates have legitimate concerns that these systems can be used for constant surveillance. In general, law enforcement does not operate that way today in the United States. However, the right approach is to provide transparency of how the biometric technology is being used by the agency through policy documents that can be shared with the public. Tools such as regular audits can provide supporting evidence that systems are being used in a manner that is consistent with agency policy.

The law enforcement professionals that make up the IACP can point to many direct and substantial public safety benefits made possible by AI-assisted biometric technologies. We are also well aware that the public has legitimate concerns about ensuring that these technologies are deployed in a way that is responsible, proportional, and respectful of civil liberties. Since these truths exist together, we support the OSTP's commitment to soliciting input from all stakeholders on how biometric technologies can best serve the public interest.

The law enforcement community has more than twenty years of experience with computer biometrics. The awareness of the limitation of the technologies has led to procedures, practices, and policies to protect both the integrity of law enforcement operations and the rights of individuals.

**Key Guiding Principles for the Use of Biometric/AI in Law Enforcement**

Any change in a technology can be difficult for an organization or group to absorb without some guiding principles to serve as a lens to evaluate and critique it. Therefore, based on previous experience, we can offer clear principles for law enforcement using these tools:

- These systems are only tools; however, they offer great efficiency improvements by automating tasks that were previously manual and yielding helpful insights and patterns that might otherwise go undetected. Automation in law enforcement should always include the important element of human verification and validation.
- Agency governance of AI technology in law enforcement must be clearly defined, codified in policy, and oversight rigorously exercised to build and preserve the public’s trust.
Accountability, in a legal sense, can only apply to human beings in law enforcement. This means an agency must own the technology they deploy. They are ultimately responsible for how it is deployed and used operationally.

The IACP has had extensive experience in applying new technology to law enforcement activities. All police agencies deploying such technologies need to document and codify the policies of use. Because of this primary need, IACP has created a formalized framework to address new technology implementations.

IACP Technology Policy Framework

As the leading professional organization for law enforcement, we seek to provide guidance to law enforcement agencies both within the United States and worldwide. Developing and enforcing comprehensive agency policies regarding deployment and use is a critical step in realizing the value that technologies promise, and is essential in assuring the public that their privacy and civil liberties are recognized and protected.

The challenges include identifying which technologies can be incorporated by the agency to achieve the greatest public safety benefits, and defining metrics that will enable the agency to monitor and assess the value and performance of the technologies. Just because a technology can be implemented does not mean that it should be. There are also challenges in integrating these technologies across different platforms, building resilient infrastructure and comprehensive security, providing technical support, and maintaining and upgrading applications and hardware. All of this can be confusing and technically demanding, underscoring the need for effective planning, strategic deployment, and performance management.

Addressing these challenges is paramount because the array of available technologies is expanding. A principal tenet of policing is the trust citizens grant police to take actions on their behalf. If that trust is violated and public approval lost, police are not able to effectively perform their duties to keep communities safe. Creating and enforcing agency policies that govern the deployment and use of technology, protecting the civil rights and liberties of individuals, and upholding the privacy protections afforded to the data collected, stored, and used is essential to ensure effective and sustainable implementation and to maintain community trust. Policies also function to establish transparency of operations, enabling agencies to allay public fears and misperceptions by providing a framework that ensures responsible use, accountability, and legal and constitutional compliance.

A short form of the key principles of the IACP Technology Policy Framework:

1. **Specification of Use** – Precisely define the intended use of all agency technology to include the agency’s detailed purpose and objectives as well as description of use that is prohibited.
2. **Policies and Procedures** – Develop appropriate and reasonable technology controls with common sense supporting procedures and guidelines.
3. **Privacy and Data Quality** – Describe how the integrity of the technology and resulting data will be ensured. Conduct both privacy and quality assessments for all employed technology.
4. **Data Minimization and Limitation** – Articulate how reasonable minimization of data collection and use is ensured and why overreach should not be a concern.
5. **Performance Evaluation** – Explain how the agency will periodically evaluate the performance and the value of the technology not only to the agency but foremost to the community.

6. **Transparency and Notice** – Design and implement technology with a reasonable ability to allow for public transparency. Even when certain data or details cannot be reasonably made public, ensure transparency of the existing controls and oversight are publicly available.

7. **Security** – Describe how the technology and related data is protected in terms of risk management and security. Ensure both positive and negative outcomes are shared with the community.

8. **Data Retention, Access and Use** – Ensure that data retention is planned with a view of the technology life cycle, minimal access and legally intended use. Plan for adequate retention to support oversight and transparency; however, preclude that data retention does not exceed acceptable and intended use.

9. **Auditing and Accountability** -- Codify enterprise-wide accountability from authorization to operate, through continuous monitoring, and regular audit of all use.

These nine principles are the base concepts that are important for any new technology to be deployed by law enforcement. Each item can be discussed extensively with any technology; however, there are considerations unique to AI.

**Specific Principles and Concerns for Biometric/AI Technology**

The principles discussed above should be used to guide development of the following areas of attention before biometric or AI technologies are deployed:

**Technology Use Policy**
Many of the biometric technologies, because they are non-intrusive, do not get the rigorous review of conditions of appropriate use. Agencies need to consider when it is appropriate to use technology in question. Many times this will/should be dictated by law and agency policy. However, because the law often takes time to catch up with technology, we can expect there will be situations that the executive and legislative branches of governments at all levels will need to weigh in.

More specific to agencies is the need to determine which personnel are authorized to use a technology. This should be a function of need, training, and certification.

**Protecting Privacy of the Public**
This is probably the most difficult aspect of Biometric/AI technology use. The public has the right to express concern about the power of government even though they freely share biometric information with social media sites, who have stated that they are using the same or even more sophisticated technology for facial recognition.

Mass image capturing and usage, such as that which is collected from red-light cameras or surveillance video, is another citizen concern. Similarly, images and data residing in popular social media systems and other publicly collected facial image repositories do not inherently violate privacy laws, but use of these image galleries by the government often leave the public very uncomfortable. Context is everything in these situations. Looking for an abducted child is going to be perceived by most of the public as an appropriate use of a public image capturing. In contrast, looking for people who
haven’t paid their parking tickets by using traffic cameras is generally not well regarded. This is further reason policy is key to guiding law enforcement staff as to appropriate and publicly acceptable usage of biometric technology.

**Appropriate Reference Data Gallery/Sources**
The gallery images (reference database of known persons/entities), especially in a facial recognition application, that should be used by law enforcement are those of a high quality. This usually means that they are collected in controlled environments, or post-processed to obtain quality without damaging the image information. Examples of this would be booking workstations when subjects are arrested and processed.

Reference data and test/probe images acquired from third party entities need to be treated as suspect and vetted appropriately.

**Security**
A quality data gallery must be adequately protected and secured as it is a prized compilation. Such a valuable data collection will attract parties interested in accessing, copying, or stealing the information. As exemplified by the 2015 hacking of the U.S. Office of Personnel Management, the combination of biometric, demographic and biographic information is of supreme interest to foreign military and intelligence agencies seeking to identify employees and personnel in sensitive roles.

**Training/Certification**
Training is a multifaceted issue. Certainly there are the basics of how to use the technology, and the need for professional and use certification when those exist. However, equally important is understanding the applicable laws, regulations, and policy that apply to the technology.

**Audits**
Audits are a common practice in law enforcement, especially in the Criminal Justice Information Systems (CJIS) environment. The CJIS environment commonly deals with criminal histories and usually will facilitate access to information regarding driver's licenses and vehicle registrations. The easy access for a sworn or civilian agency employee provides a temptation for misuse. The knowledge of an audit process can be a deterrent to bad behavior, or even uncover training and use case issues that were not clearly understood by the agency when the technology was deployed.

Furthermore, agencies need to implement Quality Management controls. These controls track the usage, success and failures of the technology. These controls start with policy statements that precisely define the intended use, avoided use, and adequate controls/oversight to ensure integrity of both.

Audits provide transparency to the public and are a key tool for law enforcement agencies to maintain community trust.

**Balancing Policy Against Use**
Ultimately, we want to ensure technologies assist officers and investigators in most efficiently solving crimes. Agencies and regulators have to be careful not to implement technology use policies that are so restrictive that the public benefits are all but diminished. Consideration should be given to balancing both risk and efficiency when developing policy. If a policy creates hurdles that make the use of
technology exceedingly difficult or impractical, end users may avoid using the tool(s), thus squandering the potential public benefit of this technology.

Any national policy recommendation on the use of AI-assisted technologies should identify the benefits of a technology as clearly and emphatically as its risks or other possible collateral impacts. The government should carefully identify and quantify the tangible public safety benefits of particular technologies, both in terms of cases solved and efficiencies realized, as well as describing potential harms. Mitigating controls should be carefully crafted to limit real and measurable abuses of the technology, rather than theoretical dangers.

Discussion of Individual AI Technologies in Law Enforcement

Our response to the RFI so far has been focused on law enforcement’s long history of biometric technology usage and the formalized method through the IACP Technology Policy Framework agencies should be using.

Artificial intelligence is currently being used in a wide variety of applications in policing today, some of which extend beyond just biometrics.

Several current and envisioned uses of AI in law enforcement include:

- **Criminal Investigative Use**
  - Automated detection of victims and perpetrators in video data from seized cell phones and computers in sexual exploitation investigations
  - Detection of objects and people in video data during criminal investigations

- **Field Operations and Criminal Investigation Use**
  - Automated facial image comparison, fingerprint comparison, retina comparison, and DNA profile comparison for lead generation in criminal investigations and identification of incapacitated individuals

- **Evidence Processing and Privacy Protection**
  - Automated redaction of sensitive objects and Personally Identifiable Information (PII) in video recordings
  - Automated removal of illicit images and videos of victims
  - Expedited review of video recordings, including videos voluntarily shared with law enforcement by members of the public

- **Training and Education**
  - Detecting law enforcement officer and private citizen sentiment in audio data of police interactions for the purposes of problem behavior detection and officer training

- **Non-Biometric Uses**
  - Automated license plate recognition and comparison for investigative lead generation
  - Remote detection of weapons using imaging radar data prior to arresting a person and during responses to people in crisis
  - Cybersecurity threat detection, mitigation, and investigation
  - Automated gunshot detection and location to reduce shooting response times
  - Recognition of patterns in criminal justice data including arrest reports, narratives, and criminal history records
In all of the applications listed above, technology is being used as a tool to gather or synthesize information for law enforcement purposes. However, similar to virtually every other police technology tool or system, AI-derived information must only be seen as a piece of evidence about criminal activity or citizen identity. The conclusions of an AI-assisted biometric system should not be understood as stand-alone proof of a particular fact. It can and should be understood as an investigative lead generation tool, and when properly corroborated and supplemented by human actors, one of the many building blocks of probable cause.

Conclusion
AI-enhanced capabilities have increased significantly during the past decade, as computing power, automated processing, and storage capacities have increased. While new public safety benefits can be achieved, challenges must be met and addressed prior to the implementation of new technologies. Police users of these systems should have a solid understanding of AI and specifically machine learning to fully comprehend both its potential positive and negative impact on the community. Failure to fully comprehend the power of biometrics and AI could leave law enforcement legally vulnerable and unaware of valid citizen concerns.

In utilizing biometric/AI applications, agencies should be cognizant of technology limitations and remain diligent in their adherence to principles outlined in the IACP Technology Policy Framework and established standards when available. Responsible use, operational transparency, protection of data, and documented verification of results will also continue to be critical for successful adoption and public acceptance of AI technologies as public safety tools - much the same way they were for the successful development and use of fingerprint systems.

Most importantly, as powerful and impressive as AI-enhanced technologies may seem, when used as investigative tools, the results they generate are only leads or starting points. Most importantly, it is the police officer, detective, investigator, or analyst who must consider that lead and corroborate it with other gathered evidence and testimony while comparing it to the requirements of law which guide our community’s behavior. Only after careful investigation and impartial human deliberation of all the facts can a decision be made to question, detain, exonerate, or arrest a person. No matter the wonderment of computer technology and its many current and future advancements, it is the trained and ethical law enforcement professional who must stand before a judge and jury to swear to the innocence or guilt of a fellow citizen. In our noble profession, we must always fight to provide justice to victims of crime and we believe that AI technologies enable law enforcement to be more effective and efficient in accomplishing that goal.

Sincerely,

International Association of Chiefs of Police (IACP)
44 Canal Center Plaza, Suite 200, Alexandria, VA 22314
Respondent Type: not-for-profit 501c(3) organization