IBIA Industry Position on Law Enforcement Uses of Face Recognition and AI

*Author: John C. Mears**

Background

Recent articles, including some published in *The Washington Post* and other national media outlets, have once again brought into question the efficacy and use of face recognition technology by law enforcement.

Face recognition, although not a brand-new technology, has been elevated to a higher level of scrutiny and controversy over the past few years, as its accuracy and its ubiquity of use have increased. Like many powerful and rapidly-evolving technologies, face recognition is widely misunderstood. Besides being used as a tool in solving crimes by law enforcement, it has the capability for a great number of other beneficial uses, particularly in facilitating air travel and border crossing, as well as employee and customer on-boarding and easing the verification and authentication process for managing physical and electronic access to sensitive and personal information. By the same token, there also exists the potential for misuse when the legal limits to the technology are not heeded, or in the misapplication of the technology, especially when undertaken by inexperienced or undertrained technicians.

Indeed, in the context of law enforcement use of face recognition, the IBIA has long held that this technology should only be utilized in the **forensic** use (that is, treated as criminal evidence acquired through scientific methods, as opposed to the use of face recognition for active **surveillance** purposes. If active surveillance is to be performed using face recognition, IBIA believes that this activity should be treated as if it were a conventional wiretap — enabled only through a court order and only to be performed for a specific time period.

One of the fundamental missions at IBIA is to educate audiences — particularly legislators and policymakers, the news media and the general public — about the wide variety of modalities and use-cases for biometric and identity technologies, as well as to address and correct misinformation and that is often promulgated by uninformed (or misinformed) sources and opponents of these technologies. IBIA's membership consists of subject matter experts who are in an optimal position to recommend responsible use-cases and applications, and throughout our history we have published industry-supported best practices and guidelines to address concerns related to the ethical use of face recognition.

**John C. Mears is a Leidos Technical Fellow, Master Solutions Architect, and Consulting Employee with current focus on border and port security, biometric traveler verification, and national-scale biometric systems. He served as Chairman of the International Biometrics and Identity Association (IBIA) for 5 years until July 2024.*

This position paper covers an industry perspective on law enforcement uses of face recognition, as well as the responsible uses of AI/ML, which is the basis for modern face recognition and related technologies.

Motivation

In May 2022, Executive Order (EO) 14074[1] outlined several wide-ranging directives aimed at enhancing public safety and improving community trust in law enforcement, which IBIA supported. Section 13 of the Executive Order directs the National Academy of Sciences (NAS) to conduct a study of current usage of Face Recognition Technology (FRT) and biometric technologies and publish a report detailing the findings. NAS empaneled a group of diverse luminaries, including privacy experts, who held hearings between May 2023 and January 2024 before publishing their report.[2] During the course of the NAS hearings, IBIA provided industry expert witnesses, and this paper represents their expressed aggregate positions.

Industry Position on Law Enforcement Uses of Face Recognition

For law enforcement other than at the federal level, we think forensic uses of face recognition for criminal activities should aways be allowed (that is, not banned) subject to the following:

- Policies stating that face recognition results of forensic investigations are only for lead generation and not dispositive by themselves;
- Supervisory level reviews of results being required;
- Case-based and periodic independent audits:
- Law enforcement users being trained;
- Access strictly limited to authorized users;
- An audit trail of usage being established;
- Penalties for misuse being established;
- An understanding of the algorithm characteristics to support confidence levels if needed for court; and,
- A commitment to sustain maintenance and cyber hygiene and perform system upgrades as technology improves.

Further, we think real-time surveillance uses of face recognition should be subject to court order, similar to that required for a wiretap, with:

- A specific legal purpose;
- A specific time period; and,
- A specific area.

Regarding federal law enforcement, we believe that federal authorities for biometrics are well specified in laws, policies and rules with details of use documented in the Federal Register, PIAs (Privacy Impact Assessments) and SORNs (System of Records Notices). In fact, we believe that the federal government is more transparent and rule-bound in this context than either the commercial segment or the state and local segment. This is why we see transparent and efficient practices such as the FBI's responsible uses of face recognition data, CBP's efficient process for inspecting international travelers at our ports, and TSA's speedy processing of trusted travelers.

However, state and local governments are far behind the federal government in terms of laws, policies, deployment, and personnel training. Even though the states are attempting to address the challenge, the developing patchwork of associated inconsistent state legislation is complex and results in compliance difficulties, especially for the commercial segment. Laws such as the Illinois Biometric Information Privacy Act (BIPA) provides for a private right of action and liquidated damages of $1000 per violation to people who are "aggrieved" by a violation of the state's restrictions on the collection, use and sharing of biometric data. In practice, the law has done little to protect the public. National legislation at the federal level is required to preempt state laws (including Illinois, California and others) and establish a uniform, safe and reasonable framework for uses of biometrics including face recognition. Biometrics should never be subject to an outright ban.

This said, the IBIA is certainly in favor of preserving rights, liberties and privacy. However, there is a distinction we should make. Privacy does not equal anonymity. It is possible to be anonymous and still have one's privacy invaded. It is also possible to retain privacy and not be anonymous. There are at least 29 federal laws defining and protecting various aspects of privacy. We found no laws guaranteeing anonymity. Criminals, terrorists and adversarial intelligence agents thrive on anonymity.

Industry Position on AI/ML

We refer to Artificial Intelligence/Machine Learning many times as "AI/ML" or simply "AI" for short. However, the applications we discuss here were created with Machine Learning (ML) technology and cannot claim to be "Intelligent" in a human sense - yet. To many people, AI technology appears to be a black box into which data are loaded, and inferences are made without explanation. Our industry has been developing technology that ensures that people or systems that use AI technology for analytics and/or lead generation can convincingly explain (e.g. in legal testimony, to a non-expert jury) how the AI technology supports their assertions and testimony. Those assertions should be fair, balanced consistent with our legal system. For example, IBIA member company Leidos has developed a Framework for AI Resilience and

Security (FAIRS) to build trustworthy AI that increases security, is predictable and resilient, and does not put humans or missions at risk.

Any biases in an AI system should be calibrated out, or at least characterized and stated, so that any derived evidence can be fairly weighed against other evidence. A well-known example of this is the FBI Combined DNA Index System (CODIS) use of population statistics (POPSTATS) to qualify the probability of a DNA match based on allele (DNA segment) frequencies in the population subgroup of the subject. Similarly for face recognition, now often based on AI/ML techniques, the assessment of demographic differentials should be provided for the algorithm and the population subgroup (demographic) of the subject. This kind of assessment has been independently done by the National Institute of Standards and Technology (NIST) as early as 2019.[3]

The best algorithms for face recognition exhibit minimal demographic differentials, and accuracies on par with fingerprint identification (i.e. 99%). The algorithms are far better and less biased than humans, who have a built-in "own race" bias.[4] Used properly, face recognition tools are a powerful force multiplier for police and other law enforcement agencies. Given budgetary constraints, and strong pushes for efficiency, police need all the advanced tools they can get for their demanding missions. However, all this pressure can lead to unintended consequences, such as skipping investigative steps or trusting a tool to operate and give accurate results autonomously without human questioning.

New AI-based systems should always be trialed with humans "in the loop" to guard against unwanted aberrations. When users gain confidence in these AI systems, particularly control systems, they should then be monitored by humans "on the loop". Only with sufficient experience and testing should such systems be considered for running autonomously (with less stringent – but still necessary – human monitoring). However, in the case of face recognition evidence used by police, there should always be at least one human, preferably two, in the loop to enforce good evidentiary practices. Face recognition searches should not be considered dispositive by themselves. They are good for lead generation but should always be backed up by other evidence before action is taken on anything as serious as an arrest. For instance, was the person who matched an image of a criminal at a crime scene even in town at the time of the incident?

Recommendation

Police agencies should voluntarily adopt the IBIA (industry) recommendations on uses of face recognition.[5] The industry cannot enforce compliance with best practices or individual police agency policies. Chiefs of police should ensure that their organizations rigorously follow

evidentiary rules, whether the evidence is face recognition or anything else. All evidence should be corroborated. Absent federal preemptive action, state and local police should enact policies and laws that enforce compliance, with appropriate penalties if rules are broken and punishment if broken rules result in improper arrests. Briefings on IBIA best practices should be given at FBI Advisory Policy Board (APB) conferences, and meetings of the International Association of Chiefs of Police (IACP), among others.

To present a complete and fair view of this topic, we highly encourage reporters to reach out to industry associations like the IBIA[6], and not rely solely on inputs from organizations blindly opposed to the technology. The IBIA has a strong interest in an active dialogue around biometrics and identification technologies and those with an interest in the policy and technical impact of biometrics or identity management should contact us directly. We are always happy to provide perspectives which advance IBIA's core mission of enhancing security, privacy, efficiency, and convenience through these technologies.

# # #

About the Author

John C. Mears is a Leidos Technical Fellow, Master Solutions Architect, and Consulting Employee with current focus on border and port security, biometric traveler verification, national-scale biometric systems, and post-pandemic travel transformation. He has testified before the House Committee on Science, Space and Technology on the "Current and Future Applications of Biometric Technologies," and served on Congressional panels addressing uses of biometrics technologies. Previously, Mears was Director of Biometrics and Identity Management for Lockheed Martin Information Systems and Global Solutions, which merged with Leidos in 2016.

Mears holds B.S.E.E. and M.S.E.E. degrees from the University of Florida and is certified as a Project Management Professional. He is an Associate Member of the American Academy of Forensic Sciences, and a member of the Biometrics Institute. He has served on several Boards of Directors and was Chairman of the Board of the International Biometrics and Identity Association (IBIA) for 5 years until July 2024.

Footnotes

[1] https://www.federalregister.gov/documents/2022/05/31/2022-11810/advancing-effective-accountable-policing-and-criminal-justice-practices-to-enhance-public-trust-and

[2] Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance | The National Academies Press

[3] Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects

[4] See Meissner, C. A. Brigham, J. C. (2001). Thirty years of investigating the own-race bias in memory for faces: A meta-analytic review. Psychology, Public Policy, & Law 7, 3–35 (providing information about human face memory across demographic groups and finding that humans remember own-race faces better than faces of people who are members of other, less familiar racial groups).

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

[6] IBIA