Members' Viewpoints: The Use of Facial Recognition in Policing

Version Final | 27 January 2025

Introduction

In late 2024, the UK Minister of State for Crime, Policing and Fire of the United Kingdom, Dame Diana Johnson, started a programme of engagement about the use of live facial recognition (LFR) by police in the absence of a single law to give the police the power to use the technology. Her aim is to ensure LFR secures and maintains public confidence. Currently LFR is governed through College of Policing guidance and existing data and privacy laws.

The Institute had the opportunity to participate in this debate and collected viewpoints from its diverse membership on the issue. Facial recognition use in public places and in particular their use by law enforcement and policing has been an important topic for discussion in the Biometrics Institute community for several years. In 2021, we published a paper asking the question: Should we ban facial recognition?

We have surveyed our members on the issue and are now publishing "Members' Viewpoints" in order to raise awareness about the following:

- The Biometrics Institute promotes the use of biometrics but only if used responsibly and ethically
- Biometrics are complex, different use cases present different levels of risk which need to be assessed, planned and managed carefully
- Missteps erode trust including those from other countries as the public suspect all such technology systems operate in the same way
- Using biometrics responsibly, requires informed decision-making, clear communication and transparency. Therefore, it's important that operations like LFR are fully transparent and are developed following the Institute's *Three Laws of Biometrics*, and *Good Practice Framework (GPF)*
- The Institute is well placed to provide these tools and accompanying guidance as the independent and impartial international membership organisation representing a diverse multi-stakeholder community from around the world, including law enforcement agencies and technology evaluation agencies, whose own experience and advice is useful

Key points

- Using biometrics responsibly requires informed decision-making. Communication, education and transparency are essential to maintain and build citizen (or public) trust in the use of facial recognition technology. Policing must be conducted with implicit public consent and trust
- There remains confusion and misinformation, often through the media and through some minority voices which are important but don't balance the discussion
- There are different use cases for facial recognition and it is important to differentiate them as they present different levels of risks and mitigation
- In policing / law enforcement the two main uses cases we see are 'retrospective/ post-event (criminal) investigations' and 'real-time (live) facial recognition' (LFR)
- For retrospective investigations the same standards and processes should apply to facial recognition that apply to DNA (robust quality management procedures (ISO/IEC 17025:2017). This is important to assure the public

- LFR worries the public, feels like a continuous police line-up. Police has always conducted live recognition of people (manual policing surveillance techniques) with officers in the street but the technology creates fear
- LFR is only indicative / speculative and should only lead to the question: Should we stop this person? Reassurances about data deletion are important. Independent testing throughout the life-cycle of the systems critical
- Private sector usage of facial recognition influences public perception. It should match the same standards and policies as police and law enforcement use as citizens will see the two use cases in the same light
- What about citizens using their own facial recognition and feeding images to the police?
- It is clear that a consistent approach to the use of FR technology is critical, and its application through well-constructed policy and process. And to make sure that all those who have an input into the use of FR within law enforcement use cases in the UK are on board with this, and understand why this consistency of approach is vital
- The *Three Laws of Biometrics* have to be front of mind: Policy first, followed by process and then the technology. We can put all the right policies in place and test the technology but we require safeguards (processes) that ensure things are managed well when something goes wrong.
- The role of UK Biometrics Commissioner was very well received by our global biometrics community. Independent oversight, guardrails and enforcement are critical success factors in delivering biometrics responsibly, ethically and effectively

Biometrics Institute Members' viewpoints

The Biometrics Institute asked its members and stakeholders to provide their views on the responsible use of facial recognition by policing and law enforcement. Their responses have been amalgamated below.

Is regulation needed?

UK-wide policy/regulation for the police use of FR is a sensible way forward because the current 'post-code lottery' of 43 Forces interpreting LFR tactics with only 'guidance' from the College of Policing is insufficient and bears the risk of inconsistent approaches. Good practice exists and should be adopted across the forces. The LFR concept can work well but it could easily be disrupted by just one Force going off script. Maybe all 43 Forces should become members of the Biometrics Institute and take advantage of the available guidance.

It seems that currently with many Forces self-designing their approach, all with differing interpretations as to what good may look like, both in terms of policy, process and technology they are using. And to add fuel to the fire they have been somewhat rushed into operating a hybrid with the national shoplifting response using unqualified CCTV systems, matching against questionable centrally held data, and now seeking to build supper CCTV command hubs taking over from the councils to have all feeds run through systems with no transparency or accountability.

Maybe it is worth considering mandatory attendance of all chief Information Officers in UK policing to attend the Institute workshops, use the *Good Practice Framework* and impose the *Three Laws of Biometrics.*

'Retrospective' usage and the effect of using crime scene images

The deployment of face recognition in criminal investigations involves the capture of face images from crime scenes (e.g. CCTV, mobile phones, dashcam/doorbell cameras etc.) that are compared 1:1 with the faces of nominated suspects or searched 1:n through a gallery of faces of convicted criminals. These comparisons/searches may result in some form of match between two images. However, the images recovered from crime scenes will be of highly variable quality in terms of

identifiable detail, pose, facial obstructions (head coverings, spectacles, masks etc.), ambient lighting etc.
Consequently, any potential matches between crime scene images and those taken under controlled conditions at police custody suites will be, in forensic science terms, subject to *a degree of uncertainty* depending on the sufficiency and clarity of identifiable detail in both images. This, in principle, is no different to the processes and challenges encountered in comparing crime scene finger marks or DNA profiles with reference fingerprints and DNA profiles obtained from arrestees. As such, this retrospective usage of face recognition and its contribution to police investigations and potential production in courts of law should be managed in the same way as fingerprint and DNA evidence namely:

1. The collection of crime scene images and the subsequent comparisons/searches and reporting of results should be conducted under robust quality management procedures (ISO/IEC 17025:2017) which will regularly test the competency of those undertaking the processes, the processes themselves and any occurrences that require corrective and preventative measures in order to maintain operating standards.
2. The production of any face recognition evidence in UK courts must be conducted by a suitably qualified and accredited forensic science expert in compliance with the requirements set out for expert witnesses in the Criminal Procedure Rules (Part 19) https://assets.publishing.service.gov.uk/media/650daab5bf7c1a0011bb4609/crim-proc-rules-2020-part-19.doc
3. These procedures must be reviewed by the United Kingdom Accreditation Service and be in the purview of the UK Forensic Science Regulator.

Live Facial Recognition in public spaces

LFR uses a gallery of face images of 'persons of interest' from police custody images (e.g. those wanted for specific offences or of other interest to police etc.) as a database. Face images of the general public are then captured in real time by cameras in a designated public space that has had warning signs erected around it e.g. a section of high street, shopping precinct, sports stadium etc. If a potential match is made then the police officers decide if it is sufficient to justify police stop of the individual in order to establish their identity and further question them if necessary.
This process has been relatively successful since its introduction and subsequent challenge in the courts. The following issues, both positive and negative in nature, are pertinent to this particular form of FR deployment:

1. LFR replicates manual policing surveillance techniques that have been employed for over a century. Police officers have been issued with face images for patrol purposes or in set scenarios (e.g. football matches) in order to spot those who may be wanted, other persons of interest, potential agitators etc. LFR just adds digital processing to this protocol but 'technophobia' and increased efficiency may have disturbed some sections of society and the media.
2. LFR is a speculative screening search and NOT a forensic investigative tool in same way as retrospective face recognition techniques. It is important to separate the two procedures and emphasise that a 'face match' in LFR does not always result in a stop or an arrest unless the identity of the individual has been confirmed by other means (e.g. mobile fingerprint device). It is intended to be indicative only. The LFR result should not used be in evidence to prosecute the data subject and if a face comparison needs to be confirmed for evidential purposes then the quality management procedures set out above for retrospective FR must be followed. The police advise that face images of the general public are captured for only a few seconds before being deleted if no potential match is made. This may be the case but it is undermined by other police practices that have resulted in the accumulation and retention of face images of those arrested but not convicted throughout the UK. This has been a continuing problem since Parliament introduced the Protection of Freedoms Act (2012) and

face images were not included as biometric material. Previously, arrestee DNA profiles had been obtained and stored in a similar fashion but the European Court of Human Rights (S v Marper) had overruled UK courts in 2008 and the practice was stopped. The public may be concerned that lessons were not learned from DNA data management and applied to face images. Therefore, reassurances about data deletion in LFR may be viewed sceptically by some even if there is no basis in reality. This lack of trust, by some, is further exacerbated by the fact that images are captured remotely and this has been presented by some critics as, in essence, a 'perpetual police line-up.'

3. The performance of face recognition algorithms has improved dramatically over the last decade and independent testing conducted by the UK National Physical Laboratory has demonstrated that the some algorithms used in LFR applications are highly accurate and exhibit little or no demographic differentials. (Query: When was the last test conducted? The Home Office Biometrics team has also conducted various evaluations of FR technology in vary recent years in a policing context. The very comprehensive work of NIST on FR is of course also highly relevant, and is publicly, freely available.
4. The face images used in the LFR gallery must be both current and relevant to the specific deployment.
5. The current state of the UK Criminal Justice System is reportedly poor with extremely long delays in court trials and UK prison capacity at maximum. Those critical of the use of LFR may question why it is deployed when the CJS is basically a 'revolving door.'

Comments on testing

It would be good to get something around the importance of ensuring systems are fit for purpose for their intended functions, which should be based on testing against internationally recognised standards by expert, independent test labs.

The Met and South Wales police forces made important steps in this direction with their NPL-led testing in 2022-23 (for info, we were partners of NPL and Tony Mansfield in that work) but it is important that such testing is not used out of context to rubber stamp the use of face biometrics in different applications. FR has the promise to provide a significant benefit to policing and to help police forces across the UK in a range of ways, and it is very important to make the most of these opportunities without undermining public confidence in their use. This is where a rigorous assurance process for the use of FR in policing is vital if it is to be used reliably and correctly.

Three Laws of Biometrics

- How is policy being developed – Are forces potentially being left to their own devices with limited central guidance?
- Same for process – and how is this being checked for optimisation – reactive vs officer initiated vs live?
- Tech and performance – central systems (PNC and its proposed successor LEDS) vs localised at force level. Police National Computer – are they setting up a centralised image database for FR? What about any governance structures being put around it - including data quality etc.
- Transparency and reporting – what data will be shared with the public, feedback and remediation.

Importance of consent, transparency, communication and guidance

- Policing in the UK is conducted with implicit public consent and trust
- Missteps erode trust and fuel various activist organisations and their specific agendas. Missteps from abroad (such as the USA LFR case presented at Biometrics Institute Congress) similarly fuel mistrust as the public suspect all such technology systems operate in the same way

- Therefore, it's important that potentially controversial operations like LFR are fully transparent and are developed following the Institute's Three Laws of Biometrics, and Good Practice Framework
- Transparent communications are always helpful in maintaining trust
- The Institute offers tools for evaluating the application of policy and the processes that can deliver policy, and for deciding on appropriate and proportionate technology
- This leads to consistent framework of functional and non-functional requirements that can be put to vendors in best practice systems engineering style
- The Institute has broad international membership support including from law enforcement agencies and technology evaluation agencies, whose own experience and advice could be useful

Regarding "demographic differentials" sometimes pejoratively called "bias":

When NIST published their analysis of demographic differential performance of face recognition algorithms, some people in the media seized on the fact that there are demographic differentials in algorithms, without understanding the magnitude and implications, especially for top performing algorithms. NIST in fact noted that for the best performing algorithms, demographic differentials were minimal.

Demographic differentials are natural and can be minimized, but will always exist. Whether they are significant or not depends on use case, magnitude of the differential, and overall accuracy and error characteristics. For forensic uses, it is important to understand the algorithm characteristics and threshold settings so we can qualify potential matches appropriately. An analogy to processes associated with matching DNA can be made, perhaps the ultimate biometric. It has long been known that the alleles in the short tandem repeat sequences used for human DNA databasing vary in frequency between demographics. These frequency differentials have been characterized for the forensic DNA community in the form of Population Statistics or PopStats. When forensic DNA examiners give the probability of a match between DNA samples, the probability is qualified and changes based on the demographic or region membership for the subject. Nobody calls this "bias". The community simply acknowledges the existence of differentials, and qualifies their work based on the known differentials. For forensic purposes, we need to evolve to this same level of maturity and scientific rigor for facial biometrics, wherein the match characteristics of the algorithms are qualified by demographic. We are all unique, and our face appearance is primarily determined by our DNA which exhibits demographic differentials. This should be embraced as natural, and agree on a way to deal with it. If Frances Collins were here, he'd probably observe that nobody has criticized God for bias due to the existence of DNA demographic differentials.

Considering algorithm accuracy is necessary but not sufficient. There are many variables that must be considered…. With few exceptions, humans are far more error-prone, and exhibit far more real bias, than the best algorithms.

Specific recommendations regarding uses by law enforcement:

For law enforcement…:

- Forensic uses of face recognition for criminal activities should aways be allowed (that is, not banned) subject to:
    - 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:
    - Police 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 as discussed earlier to characterize confidence if needed for court; and,

    - A commitment to sustain maintenance and cyber hygiene, and perform system upgrades as technology improves.
- Real-time surveillance uses of face recognition should be subject to court order, similar to that required for a wire tap, with:
    - A specific legal purpose;
    - A specific time period; and,
    - A specific area.

Regarding face recognition and societal benefits and acceptance:
Addressing … impacts of face recognition, advancements in the field have resulted in technology that is approaching the accuracy of fingerprints under the right conditions. Our passage through airports and international ports of entry is becoming faster, more hygienic and touchless for identification purposes. In a 2022 survey of over 10,000 people from 222 countries by the International Air Transport Association, 75% would rather use biometrics than passports for identification, a testament to their usability and popularity. Use of facial recognition as an option for taxpayers with the U.S. Internal Revenue Service (IRS) has resulted in their identity verification numbers going from 44% to 78%. This means that their service to taxpayers improved by 77% over the prior performance baseline which used knowledge-based authentication.

Regarding rights, liberties and privacy:
However we may use face recognition, we are all in favor of preserving rights, liberties and privacy. However, there is one 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. <In the U.S.> The last time we counted, there were 29 federal laws defining and protecting various aspects of privacy. We found no laws guaranteeing anonymity, nor should there be in a law-abiding society.

Further considerations

The following links may be of interest to gain an understanding of the work going on in various police forces with facial recognition and in particular LFR.

CONNECT NEW YORK
This is a public safety programme enabling the people of New York City to help keep their community safe.
https://newyorkcityconnect.org/

Live Facial Recognition: How does it work? Metropolitan Police in the UK
https://www.youtube.com/watch?v=oRGu_aK9TEo

Implementation of DHS Directive 026-11: Use of Face Recognition and Face Capture Technologies in the US
https://www.dhs.gov/sites/default/files/2025-01/25_0117_cio_Report-Select-Use-Cases-2024_Final-508.pdf

The Biometrics Institute *Good Practice Framework (GPF)*
In 2020 the Institute published the *GPF*, a first-of-its-kind good practice tool that outlines the stages of the **strategic planning, procurement and operation** of a biometric system or network. It is a risk management tool helping with the decision-making process when implementing biometrics.

As every biometric use case and related policy is different, we offer tailored in-house workshops. **Your specific use case or organisational context for biometrics will be reviewed against the GPF to determine questions and issues relevant for your circumstances.** You can find out more by contacting us.

The Institute offers a range of educations tools and more information is available from our website.

About the Biometrics Institute

The Biometrics Institute is the independent and impartial international membership organisation for biometric users and other interested parties. It was established in 2001 to promote the responsible, ethical and effective use of biometrics. It has offices in London and Sydney.

The Institute represents a global and diverse multi-stakeholder community of close to 200 membership organisations from 41 countries. While a large proportion of the members are from government, other members include banks, airlines, biometric experts, privacy experts, suppliers, academics and 18 Observers representing United Nations agencies, IGOs and European Union institution.

The Biometrics Institute connects the global biometrics community. It shares knowledge with its members and key stakeholders and most importantly, develops good practices and thought leadership for the responsible, ethical and effective use of biometrics.

For more information, visit www.biometricsinstitute.org

Contact:
Isabelle Moeller
Chief Executive
Biometrics Institute
isabelle@biometricsinstitute.org
Tel +44 7887 414 887

Dated: 27 January 2025