SCOTTISH POLICE AUTHORITY
ÙGHDARRAS POILIS NA H-ALBA

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Discussion Paper on the Potential Adoption of Live Facial Recognition by Police Scotland

Contents

Introduction

At the first Scottish Biometrics Conference in June 2024, the Chair of the Scottish Police Authority launched a national conversation on the potential use of Live Facial Recognition (LFR) in a Scottish context.

This tripartite conversation, being led by a Short Life Working Group (SLWG) including Police Scotland, the Scottish Police Authority and the Scottish Biometrics Commissioner, aims to understand the public and key stakeholders' views on the possible adoption of LFR in Scotland in certain circumstances. These views are sought prior to any decision being made on whether Police Scotland expend resources on exploring LFR in detail.

Alongside this paper, there will be exploratory conversations and surveys with key stakeholders and representative organisations. It is hoped that the partners can produce videos to support discussion on LFR. The purpose of these activities is to gain initial insights from the wider public as to their views on the use of LFR by Police Scotland. The evidence gathered from the national conversation will be used to inform a position how Police Scotland may or may not proceed in exploring the use of LFR.

This paper aims to provide a summary of the available information on the use of LFR in a policing context. It sets out what LFR is and how it has been applied by policing in England and Wales, potential use cases on where it may be useful in Scotland, the legislative context in which LFR would operate in and the human rights and ethical considerations.

What is LFR?

Facial Recognition technology uses Artificial Intelligence (AI) to identify individuals in a digital image (such as a video or photo). This technology relies upon an algorithm which is trained to detect what a face is, and will then be trained to recognise faces and to distinguish one facial image from another. It does so by measuring distinguishable features of an individual's face. This creates a unique code, known as a 'face print' or 'biometric template' from a photo or video. Live Facial Recognition (LFR) uses this technology to assess real-time, live video footage of crowds who are passing a camera and automatically compares the images of those in the crowd against a database of people on a predetermined database of images, known as a watchlist. Appendix A provides further detail on how LFR is used in a policing context.

The Home Office stipulates that all uses of LFR by policing must be intelligence-led, targeted, time-bound and geographically limited. If there is an alert from the software to suggest a match, the decision to proceed, based on proportionality and necessity in the specific circumstances, will always be made by a police officer, using their professional judgement. That officer is naturally accountable for their decision making and any course of action followed thereafter.

Benefits and limitations

LFR is used in the private sector, in particular by major retailers. Research has shown that individuals are more likely to trust the use of LFR by police (79%) and the National Health Service (66%), as opposed to private companies, such as retailers (38%).

LFR is used to replicate officers watching a crowd to identify wanted or missing people. It is argued the technology is quicker, more accurate and releases officer capacity for use elsewhere. In addition, it is argued that LFR provides the benefit of being able to apprehend subjects in circumstances where this may not be possible, and when it may have otherwise taken a considerably longer period of time and resource.

LFR has also been noted for its potential to act as a deterrent to criminal activity. It may be used to tackle specific crime types, including knife crime. It is also argued that LFR will improve safety, particularly for women and girls, through the prompt identification of persons who may be wanted, or have court imposed conditions, and who may pose a threat to them.

South Wales Police explain that LFR is:

"…an efficient and effective policing tactic to prevent and detect crime, and protect the most vulnerable in our society."

Appendix B provides further detail on UK government views and funding in support of LFR.

Public polling on the use of emerging technologies

In 2022, the Scottish Biometrics Commissioner commissioned a report into public attitudes on the police use of biometric data. Though not specifically relating to LFR, this report found 66% agreed that police should use facial recognition technology in public spaces to identify those wanted by the police. The Authority has commissioned further polling to provide an update to this polling, however the results of this polling are not available at time of writing.

Further polling has included trend analysis to determine the Scottish public's perception on the use of technology. Of particular relevance is that more people feel the benefits outweigh the risks in regards to 'Facial recognition computers which can learn identities through CCTV video to catch criminals' compared to those who feel the risks outweigh the benefits. This saw a decline from 32% in 2020 to 20% in 2022. However, 75% of respondents were in favour of police adopting LFR.

Research has found that 60% of the public reported that they were 'comfortable' with police use of identification biometric systems (such as facial recognition in crowded spaces to identify suspects). However, if LFR is used in other contexts, this level of comfort may increase or decrease.

Concerns around the use of LFR in policing have centred on the capabilities of the technology, the legal framework and the disproportionate impact of LFR on the right to privacy. These are discussed in more detail in the Human Rights and Ethical Considerations section.

Use of LFR in policing to date

For policing in England and Wales, LFR is typically deployed using vans with LFR cameras. Clear signage is on both the vans and throughout the area to advise the public that LFR is in operation. Operational staff are also in the area to monitor any alerts received and are available to be approached by members of the public should they have questions. In addition, the police should inform the public of any deployments via its website or social media platforms. The results of LFR deployments are also published by police forces.

Potential Use of LFR by Police Scotland

The implementation of LFR by Police Scotland must support the delivery of key strategies, priorities and plans, including:

- Strategic Police Priorities
- Joint Strategy for Policing 2023
- Violence Against Women and Girls Strategy 2023

As noted previously, LFR may compliment traditional policing techniques. In particular, it may be used where the benefits are proportionate and necessary in balancing the rights and collateral intrusion of an individual, with keeping the public safe. This can be applied by prioritising high-risk/high-harm incidents or individuals, with risk assessments considered on a case-by-case basis for all other potential deployments.

The SLWG propose any considered use of LFR is guided by a set of 'Principles for Use' as part of a detailed Live Facial Recognition Policy.

The key focus of the SLWG was to consider and evidence “Use Case” examples of how LFR can be applied to Scottish policing. Workshops were held with key Police Scotland business areas including the Chief Data Office, Local Policing, Intelligence and the Policing in a Digital World programme. Three such “Use Cases” are outlined below:

Use Case 1 – City/Town Centre Nightlife	**Potential Public Safety and Policing Benefits Realised**
Deployment of LFR, during specific timeframes, in populated areas where analysis has highlighted heightened threat, where perpetrators target females and there is a risk of sexual or violent altercations.	Prevention - deterrence effect, minimising the risk of offending in the area of the deployment. Protecting women and girls from the risk of harm. Public Confidence - enhancing public confidence in Police Scotland's commitment to tackling Violence Against Women and Girls (VAWG). Detection of offenders - identifying perpetrators who are wanted or in breach of court orders, bringing them to justice prior to the commission of additional offences. Efficiencies - the use of technology maximises efficiency, enabling officers to focus on a greater range of policing priorities to promote public safety. Additionally, early identification and intervention would mitigate subsequent costs in public inquiries should a significant adverse incident occur. Effectiveness - technology is more likely to successfully process significant volumes of data to identify and safeguard people in large groups with less concern about human limitations e.g. fatigue, incapacity to physically scan and recognise individuals amongst hundreds of people.

Use Case 2 – High Risk Missing Persons (e.g. young children, vulnerable persons, i.e. elderly, dementia sufferers, etc.)	**Potential Public Safety and Policing Benefits Realised**
Deployment of LFR, e.g. at transport hubs, or where intelligence supports a likely location, to expedite Police Scotland's ability to safeguard and support vulnerable or missing persons.	Public Safety / Safeguarding - identifying and locating vulnerable individuals prior to them coming to harm. Public Confidence - successful location of subjects and protection of their ECHR Article 2 Right to Life / prevention of offending in a timely manner will support or enhance public confidence in the police. Expediting identification of potential offences and detection of offenders e.g. where the person located is subject of human trafficking or child sexual exploitation. Efficiencies - the use of technology maximises efficiency, enabling officers to focus on a greater range of policing priorities to promote public safety. Additionally, early identification and intervention would mitigate subsequent costs in public inquiries should a significant adverse incident occur. Effectiveness - technology is more likely to successfully process significant volumes of data to identify and safeguard the people in large groups with less concern about human limitations e.g. fatigue, incapacity to physically scan and recognise individuals amongst hundreds of people.

Use Case 3 – Largescale Indoor Events	**Potential Public Safety and Policing Benefits Realised**
Deployment of LFR at indoor events where large numbers are expected to identify known individuals who pose a risk to public safety, potential acts of terrorism, or those subject to bail conditions or restriction orders preventing their attendance at the event (e.g. RSOs, Counter Terrorism watchlists, etc.).	Public Safety / Safeguarding - identifying, locating and arresting those who pose significant risk to attendees i.e. Registered Sex Offenders, Counter Terrorism subjects of interest etc. Prevention - the known presence of LFR will have primary and secondary prevention benefits. Public Confidence - successful location of those who pose a risk to attendees will support or enhance public confidence in the police. Efficiencies - the use of technology maximises efficiency, enabling officers to focus on a greater range of policing priorities to promote public safety. Additionally, early identification and intervention would mitigate subsequent costs in public inquiries should a significant adverse incident occur. Effectiveness - technology is more likely to successfully process significant volumes of data to identify and safeguard the people in large groups with less concern about human limitations e.g. fatigue, incapacity to physically scan and recognise individuals amongst hundreds of people.

The Legislative and Regulatory Framework in Scotland

The Police and Fire Reform (Scotland) Act 2012 outlines the role and duties of Police Scotland and the Scottish Police Authority.

There is no single piece of legislation for the use of LFR in Scotland (or the UK). Any use of the technology would therefore be regulated by the following legislation:

- Human Rights Act 1998
- Equality Act 2010
- UK General Data Protection Regulation
- Data Protection Act 2018

This would be supported by the Scottish Biometric Commissioner's Code of Practice and in line with guidance on law enforcement use of LFR by the Information Commissioner's Office (such as a Commissioner's Opinion on use of LFR in public spaces and good practice checklists)

Any use of LFR will need to have a legal basis that is sufficiently clear and foreseeable and have to adhere to these pieces of legislation and codes. The common law (i.e. non-statutory sources of law such as case law) may also form part of the legal framework, particularly where this concerns the nature and extent of police powers.

There would also be a need to provide a detailed overview and analysis of any equalities, human rights or data protection implications of LFR, the completion of an Equality Impact Assessment (as noted in the Equality Act 2010 (Specific Duties) (Scotland) Regulations 2012). For more specific information on the implication son the Human Rights Act 1998, Scottish Biometrics Commissioner Code of Practice, equality and data protection considerations please see Appendix C.

Human Rights and Ethical Considerations

Efficacy and Accuracy

A review of LFR usage by Metropolitan Police Service (MPS) found that between January and June 2024, 500 hours of surveillance footage was captured. Further analysis of the 79 deployments conducted in this timeframe found that police stopped one person every 55 minutes, with an arrest every 128 minutes. The review, conducted by Stopwatch, concluded that there was limited evidence of the efficacy of LFR.

Big Brother Watch has published findings raising concerns around the accuracy of LFR. Published in 2018, this report found that the use of LFR by MPS has a 98% accuracy rate, and that South Wales Police (SWP) LFR has a 91% accuracy rate. However, the Biometrics Institute concluded that there was insufficient data in this report to assess the accuracy of LFR.

In addition, it should be noted that the quality of images in watchlists may impact LFR's accuracy. This may be counteracted by the existence of International Organization for Standardization (ISO) Accreditation (ISO/IEC 19794-5) which details the standards of images that should be used in a watchlist database. Whilst this standard exists for the quality of images, there is no specific ISO accreditation for the overall standard of LFR technology, which requires the need for human decision-making on its outputs.

Police Scotland will require to ensure that images taken in custody or obtained from other sources such as CCTV, are of sufficient quality to maximise the effectiveness of any future technologies adopted.

Differing technologies have varying standards and thresholds for quality, and Police Scotland are already reviewing and improving the resolution of images captured in custody to ensure future compliance.

Bespoke weeding policies would be applied in line with relevant policy and legalisation to ensure regulatory compliance. This may be monitored through periodic review and reconciliation exercises with national databases which will also ensure data is accurate and available for searching.

Human rights and the use of LFR

Police use of LFR has raised concerns and debate in relation to privacy, civil liberties and ethics. The privacy organisation Big Brother Watch has an active campaign against the use of LFR in the UK, and has previously highlighted concerns regarding the lack of legal framework governing its use, arguing that police have no clear lawful basis to use LFR. Liberty, the civil rights group, has also campaigned against the police use of LFR, and provided the legal support to the aforementioned Bridges v South Wales Police court case.

Some have highlighted their concerns about the potential "chilling effect" of LFR and its potentially negative impact on democracy and freedom of expression. This could be through individuals choosing to avoid public assemblies and the use of public spaces by some communities.

The Justice Sub-Committee of the Scottish Parliament published a briefing in February 2020 discussing the use of LFR by in a Scottish policing context. This briefing stated its belief that:

> *"The use of live facial recognition technology would be a radical departure from Police Scotland's fundamental principle of policing by consent"*

The Sub-Committee also noted its expectation that a thorough and transparent review of necessity and accuracy, alongside an assessment of the impact on communities and individuals, would be conducted prior to any decision to implement this technology. However, following the Scottish Biometrics Conference in June 2024, the Scottish Government emphasised that any decision to use LFR is an operational decision to be made by Police Scotland.

Biases in technology

One of the key concerns that has been raised in relation to Facial Recognition technology in general is the potential for bias in the algorithms used. These have historically been proven to be less accurate at detecting and matching faces of certain skin tones and genders compared to others, often resulting in discrepancies in true positive or false positive matches across different demographics. This bias can be the result of limitations in the AI model itself, often in cases where the data that has been used to "train" the model does not offer a truly representative sample of society. This can lead to the AI being inherently biased towards specific types of faces.

An independent audit by the University of Cambridge's Minderoo Centre for Technology and Democracy in 2022 found that UK police deployments of LFR had failed to meet minimum ethical and legal standards. This was due to the deployments being too broad in scope and therefore infringing upon the privacy rights of the public. The audit also found that neither the MPS nor SWP had transparently evaluated the LFR tool they used for any bias and had failed to demonstrate that there was always a "human in the loop" - a human operator who assesses and verifies any facial matches identified by the technology.

Following this audit, the MPS and SWP published the results of testing that was carried out on their Facial Recognition Technology by the National Physical Laboratory (NPL). This provided a better understanding of the demographic performance of the LFR system and established that there are settings that the algorithm can be operated at where there is no statistical significance between demographic performance. For more information on the findings from this report please see Appendix D.

It is accepted that the most effective mitigation to prevent any false identifications is to ensure there is a "human in the loop" to verify what the technology is providing as a potential match. However, some argue that human decision making will also bring challenge and bias. Continual testing and evaluation are also required to properly assess how well the technology performs in real-life situations.

Transparency and Proportionality

There is a legal and moral obligation to inform members of the public that LFR is in operation. Forces in England and Wales have therefore used clear signage in areas of deployment to make all passers-by aware that the technology is currently being used.

Data Protection Impact Assessments completed by MPS and SWP also state that they minimise the amount of personal data being processed during LFR deployments by ensuring that any captured images that are **not** matched to the watchlist are deleted immediately.

Both MPS and SWP also publish their Facial Recognition policy documents, impact assessments and records of deployment online for open access. Having an open record of usage and clear policy around LFR has been recommended by the College of Policing as a means of ensuring that use is limited to specific deployments, which are necessary and proportionate to fulfil a legitimate law enforcement or public safeguarding purpose.

The research and consultancy firm Gartner have also published guidance around the ethical and responsible use of LFR. They highlight that LFR should be used for "specific, deliberate, predefined purposes" and organisations may encounter ethical issues if they deviate from these original purposes. The Biometrics Institute also stresses the importance of ethical use of any biometric technology. In particular, this should include public consultation and transparency to maintain public consent and trust when LFR use is being considered in a policing context.

Safeguards around the use of emerging technologies

UK police forces have been open to criticism for failing to ensure independent oversight of new technology such as LFR. The National Police Chief's Council (NPCC) is currently developing a nationwide strategy for responsible use of AI, leaning on the expertise of academics outside of policing. West Midlands Police have also established their own Ethics Committee to allow for independent assessment of new technologies in policing.

To support a consistent adoption of LFR across policing, the College of Policing has published Authorised Professional Practice (APP). This guidance explains that any use of LFR in policing must be supported by a comprehensive suite of policy documents, considerations relating to protected characteristics and detailed guidance on how police should generate watchlists.

Governance of emerging technologies by Police Scotland

Police Scotland have measures in place to safeguard emerging technologies. In 2023, Police Scotland and the Scottish Police Authority approved the introduction of the 'Rights Based Pathway' to support decision making and maintain public trust in the organisation when adopting new technology. The Pathway puts the examination of ethical issues and public engagement considerations at its heart.

Police Scotland's Data Ethics Framework and triage process is an integral part of the Rights Based Pathway and has been developed to ensure that there are formal mechanisms to seek further internal and independent advice, challenge and scrutiny as necessary.

Governance of Biometric Data

Police Scotland have robust governance measures in place in respect of biometric data. Strategic oversight is provided by the Biometrics Oversight Board, led by the Assistant Chief Constable Major Crime, Local Crime and Public Protection. Board members include the Scottish Police Authority, the Scottish Biometrics Commissioner and the Scottish Government.

Police Scotland have also introduced a dedicated Biometric Data portfolio to strengthen internal governance assurance across biometric data. This includes ensuring weeding is applied in accordance with legal timeframes, as well as routine data quality and assurance reviews.

Conclusion

The purpose of this paper is to collate information to provide an overview of what LFR is, how it can and has been used in policing, the legislative and regulatory framework around LFR and potential ethical issues impacting the implementation of LFR by police forces.

This paper is intended to aid stakeholders, members of the public and senior leaders in policing to understand LFR and its potential use in a Scottish policing context in more detail.

Appendix A: Using LFR in a policing context

Live Facial Recognition (LFR) uses this technology to assess real-time, live video footage of crowds who are passing a camera and automatically compares the images of those in the crowd against a database of people on a predetermined database of images, known as a watchlist. The College of Policing provides guidance to police to ensure that watchlists are intelligence based and proportionate. It is important that these watchlists remain current and relevant to deployments.

The technology will compare these 'face prints' with those of individuals on this watchlist. If the resultant image is sufficiently similar to one held in the database, then an alert is created and sent to the operational staff in the area to enable a decision to be made as to whether the individual should be engaged with. Following a decision to proceed, the standard investigative procedures will be followed. Images that do not raise an alert are automatically and immediately deleted.

LFR has many potential uses. The Information Commissioner highlights several including advertising (e.g. estimating footfall in advertising space, measuring engagement with advertising space), age estimation when buying restricted goods or entering age-restricted premises, and queue time monitoring and management in airports. Currently LFR is **not** deployed as part of policing in Scotland, however, it was first used by policing in England and Wales in 2017.

Appendix B: UK Government views on LFR

In October 2023, then Minister for Crime, Policing and Fire wrote to Chief Constables and Police and Crime Commissioners to note the support of the UK Government with regards to the use of LFR. To support this stance, the Minister noted that recent LFR deployments "led to arrests that would otherwise have been impossible" as "no number of officers could have picked those people out of a crowd".

Furthermore, the UK government committed to investing £55 million to introduce LFR in policing in England and Wales. This investment is in pursuit of saving 38 million hours in police time overall by investing in technology. Following a UK Parliament debate on the use of LFR in November 2024, the policing minister highlighted that LFR could be "transformational" for policing, but also recognised the impact of LFR on human rights and individual privacy.

Appendix C: Detail on the legislative and Regulatory Framework in Scotland

Human Rights Act 1998

The Human Rights Act 1998 incorporates into UK law the rights contained in the European Convention on Human Rights.

The use of LFR will invariably engage Article 8 of the Convention (the right to respect for private and family life).

Article 8 provides:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 8 is what is known as a "qualified" right, which means that public authorities may lawfully interfere with the right if certain conditions are satisfied. These conditions are as follows:

- The interference must be "in accordance with the law" i.e. it must have some basis in domestic law. The provision in domestic law must be accessible (i.e. published), sufficiently clear, and its effect must be reasonably predictable.

- The interference must pursue a legitimate aim, such as public safety, the prevention of disorder or crime, or the protection of the rights and freedoms of others.

- The interference must be "necessary in a democratic society", meaning -

    - that there must be some "pressing social need" for the interference: is the need sufficiently important to justify limitation of a fundamental right?

    - that the intrusion into fundamental rights must be proportionate to achieving the legitimate aim: any interference must not go beyond what is considered necessary to achieve the aim.

The use of LFR may also engage other Convention rights such as Article 2 (the right to life); Article 10 (freedom of expression); and Article 11 (freedom of assembly and association).

Article 2(1) provides that everyone's right to life shall be protected by law. This includes a positive obligation on the state to take reasonable steps to protect individuals where there is a real and immediate threat to life. In the context of LFR, such an obligation may arise where e.g. a person identified is known to pose a real and immediate threat to the lives of those in the vicinity.

Article 10, another qualified right, provides that everyone has the right to freedom of expression. Article 10 rights may be subject to restrictions which are prescribed by law and are necessary in a democratic society, in the interests of e.g. national security, prevention of disorder or crime and for the protection of the rights of others.

Article 11, also a qualified right, provides that everyone has the right to freedom of peaceful assembly and to freedom of association with others. Any restrictions on Article 11 rights must be prescribed by law and necessary in a democratic society, in the interests of e.g. national security or public safety, for the prevention of disorder or crime, or the protection of the rights and freedoms of others. Article 11 does not prevent the police from imposing lawful restrictions on exercise of these rights.

Articles 10 and 11 may be engaged where e.g. LFR is to be used in policing an assembly or demonstration where there is considered to be a risk to public safety from specific individuals.

Equality Act 2010

Under section 149 of the Equality Act 2010 public authorities (including Police Scotland) must have due regard to the need to:

(a) eliminate discrimination, harassment, victimisation and any other conduct prohibited by the Act;

(b) advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it; and

(c) foster good relations between persons who share a relevant protected characteristic and the persons who do not share it.

This is known as the Public Sector Equality Duty (PSED).

In the context of LFR, concerns have been expressed that some facial recognition software can give rise to a greater risk of false identifications among those from black, Asian and other minority ethnic backgrounds, and also women.

Accordingly, before using LFR, a public authority will need to satisfy itself that the particular software does not have a material bias in relation to race or sex.

Data Protection Act 2018

There are additional requirements for data protection that must be considered in the use of LFR. Part 3 of the Data Protection Act 2018 sets out the data processing requirements for law enforcement purposes (meaning for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security).

LFR collects biometric data. Biometric data relates to: "personal data resulting from specific technical processing [1] relating to the physical, physiological or behavioural characteristics of a natural person [2], which allow or confirm someone's unique identification of that natural person, such as facial images or dactyloscopic [fingerprint] data [3]."

Processing of biometric data requires additional conditions to be met, as this is considered to be sensitive processing. Sensitive processing must only be completed in "strictly necessary" circumstances or where the data subject consents. "Strictly necessary" requires robust justification for the processing of this information. According to guidance from the Information Commissioner's Office, this means that consideration should be given to:

- ensure that the processing of sensitive information is specific in nature and dependent on the specified law enforcement purpose;
- clearly demonstrate why there are reasonably no less intrusive means of achieving the same purpose; and
- clearly demonstrate how such processing will be effective in meeting the specified law enforcement purposes.

Schedule 8 of the Act has the following provisions sensitive processing:

- Judicial and statutory purposes - for reasons of substantial public interest
- Administration of justice
- Protecting the vital interests of the data subject or another individual
- Safeguarding of children and of individuals at risk
- Personal data already in the public domain (manifestly made public)
- Legal claims
- When a court acts in its judicial capacity
- The purpose of preventing fraud
- Archiving, research or statistical purposes

Data (Use and Access) Bill

The Data (Use and Access) Bill, introduced to the House of Lords in October 2024, includes provisions related to AI and is applicable in Scotland. Specifically, the Bill addresses automated decision-making systems which often use AI. Under this Bill, automated decision making is generally permitted, provided safeguards are implemented. The safeguards must allow individuals affected by such decisions to make representations, obtain meaningful human intervention and challenge solely automated decisions.

This is likely most relevant in areas similar to Automatic Number Plate Recognition, where there is the potential for this to be expanded to check if drivers are using phones or are distracted, for example. There would most likely need to be a human check of the image before a fixed penalty notice is sent.

At time of writing, the Bill is at the Committee Stage in the House of Parliament.

Bridges v Chief Constable of South Wales Police

In August 2020, the Court of Appeal in England and Wales ruled that the use of LFR by South Wales Police (SWP) was unlawful. The judgment overturned an earlier decision by the High Court in which the use of the technology had been considered lawful.

Below is a summary of the key points in the Court of Appeal's judgment.

- The use of LFR breached Article 8 of the Convention because the interference was not in accordance with the law. Specifically, SWP's policies were not sufficiently clear on who might be placed on the watchlist, or on the criteria for deciding where LFRR can be deployed. The court considered that a crucial part of the legal framework was the instantaneous and automatic deletion of images that do not match images on the watchlist. However, the policies did not make clear that this feature of the software was essential.

- The High Court did not make an error in deciding that SWP's use of LFR on the occasions in question was a proportionate interference with Article 8 rights. The High Court found that SWP had used LFR in an open and transparent way, for a limited time, and for a specific and limited purpose. In the High Court's view, neither of the LFR deployments it considered had resulted in a disproportionate interference with Article 8 rights.

- SWP had not taken reasonable steps to satisfy the PSED. Specifically, SWP had never sought to satisfy itself that the particular software did not have an unacceptable bias in relation to race or sex. While no evidence was presented to the court that the software used by SWP had these deficiencies, the court referred to evidence that some LFR software can have such a bias.

Scottish Biometrics Commissioner Code of Practice

The Scottish Biometric Commissioner's Code of Practice also sets out guiding principles on the use of biometric data. Referencing the Scottish Biometrics Commissioner Act 2020, biometric data is defined as:

"… information about an individual's physical, biological, physiological, or behavioural characteristics which is capable of being used, on its own or in combination with other information (whether or not biometric data), to establish the identity of an individual.

For the purposes of subsection (1), "biometric data" may include:
a. Physical data comprising or derived from a print or impression of or taken from an individual's body,
b. A photograph or other recording of an individual's body or any part of an individual's body,
c. Samples of or taken from any part of an individual's body from which information can be derived, and
d. Information derived from such samples."

The Code of Practice applies to the acquisition, retention, use and destruction of biometric data by Police Scotland, the Scottish Police Authority and the Police Investigation and Review Commissioner.

In addition to referencing the applicable legislation noted in this paper, the Code of Practice is informed by 12 principles and ethical considerations:

- Lawful authority and legal basis
- Necessity
- Proportionality
- Enhance public safety and public good
- Ethical behaviour
- Respect for the human rights of individuals and groups
- Justice and accountability
- Encourage scientific and technological advance
- Protection of children, young people and vulnerable adults
- Promoting privacy enhancing technology
- Promote equality
- Retention periods authorised by law

Information Commissioner's Office - Data Protection Reminders

To support the use of LFR in law enforcement, the Information Commissioner's Office (ICO) has published an summary of considerations that must be made prior to its implementation.

Firstly, it must be strictly necessary with regards to the Data Protection Act 2018, as noted above. There must also be a clear purpose for the use of LFR under this legislation.

Law enforcement must also complete appropriate documentation, including a Data Protection Impact Assessment, an Appropriate Policy Document and should develop local policies and procedures to support the use of LFR.

The effectiveness of LFR must also be demonstrated to support the proportionality and strict necessity of LFR use. The ICO emphasises that the use of LFR to meet specific law enforcement purposes must be clearly explained. The inclusion of any images on watchlists must be subject to enhanced considerations and care with regards to processing, and any watchlists should adhere to data protection principles.

The ICO also suggests that information on deployments and the contact details of the controller should be available to the public. Law enforcement agencies should also consider how the public can be provided with information as to how they exercise their rights.

Finally, any technology should be reviewed and tested on a periodic basis to assess its accuracy and effectiveness.

Appendix D: National Physical Laboratory (NPL) review of MPS and SWP LFR technology

MPS and SWP use NEC Neoface V4 facial recognition software which has a 0.6 facial matching threshold. The threshold relates to how many aspects of the image captured and the image in the database are compared and the volume of matches between them required to result in a positive identification. Uses by MPS include "to prevent and detect crime, find wanted criminals, safeguard vulnerable people, and to protect people from harm". SWP state they use LFR to "prevent and detect crime and help protect the vulnerable" - see Box 2 for recent examples of LFR deployment.

Box 1

True-Positive Identification Rate (TPIR) - the rate of successful recognition when people on the watchlist pass through an area with LFR cameras.

False-Positive Identification Rate (FPIR) - the rate of incorrect recognition (i.e., false positives or false alerts) when people not on the watchlist pass through an area with LFR cameras.

For a watch list containing 10,000 images (more in line with the size of MPS lists), there was a TPIR of 89% and a FPIR of 0.017 (1 in 6000). For a watch list containing 1,000 images (more in line with the size of SWP lists), there was a TPIR of 89% and a FPIR of 0.002 (1 in 60,000).

In relation to demographics (ethnicity, gender, age and height), it was found that:

- TPIR improved with age
- TPIR and FPIR at a face-matched threshold of 0.6 was equitable across gender and ethnicity groups.
- How crowded areas are where LFR cameras are in operation can impact TPIR in relation to height.

Box 2: Examples of uses of LFR in policing in England and Wales from Home Office Police use of Facial Recognition: Factsheet

At the Arsenal v Tottenham north London derby on 24 September 2023, it led to three arrests, including a suspected sex offender.

A wanted sex offender was sent back to jail after being identified at the Coronation of King Charles. An image of his face matched that of a wanted suspect. He was arrested and sent back to prison for breaching the terms of his release.

Over two Friday nights in Soho in August 2023 the MPS used it to help find high harm offenders. Across the two deployments there were six accurate alerts and no false alerts. It led to the police engaging with six people, five of whom were arrested including a man wanted for possession of a bladed article and a woman wanted for breach of bail in relation to robbery.

This review concluded that the accuracy of LFR had significantly improved. The technology behind LFR, as with any new technology, continues to improve gradually in terms of accuracy and efficiency.