February 2026

Response to Consultation on a new legal framework for law enforcement use of biometrics, facial recognition and similar technologies

Introduction

CEMVO Scotland is a national intermediary organisation and strategic partner of the Scottish Government Equality Unit. Our aim is to build the capacity and sustainability of the ethnic minority (EM) voluntary sector and its communities. Since being established in 2003, we have developed a database network of over 600 ethnic minority voluntary sector organisations throughout Scotland to which we deliver a wide range of programmes that provide capacity building support to the sector.

As a national organisation, we continually engage with the EM voluntary sector and its communities, which enable us to gather intelligence about the needs and issues affecting the sector. This helps our organisation to deliver tailored support to the sector, and to work strategically with public, statutory, and government agencies to tackle a range of prevalent issues such as race equality, social inclusion, capacity building and civic participation.

One of our core programmes at CEMVO Scotland is Race for Human Rights. The aim of this programme is to help public service providers in Scotland increasingly embed race equality and human rights in their strategic planning and day-to-day functions. This will be achieved by adopting an anti-racist and human rights-based approach.

Key summary of CEMVO Scotland's position

Having outlined our principles as an organisation, we are deeply concerned that the use of discriminatory and racially biased technologies would cause a detrimental impact on visible ethnic minority people and communities who already experience disproportionate impacts of racism in various aspects of life. Different parts of the UK where live facial recognition (LFR) technology was deployed saw cases of seriously inaccurate results, such as Shaun Thompson, an anti-knife crime activist, who was

misidentified and wrongly stopped by police in London[1]. As of writing, Mr Thompson is being supported by Big Brother Watch in a legal challenge against the Met Police[2].

CEMVO is a charity that operates in Scotland, and it is important to note that while we are responding to the UK Government's consultation regarding the new legal framework for biometrics, facial recognition and similar technologies, we remain firm in advocating for race equality and human rights in Scotland and across the UK. We welcome that the Scottish Parliament's Justice Sub-Committee on Policing stated in 2020 that "there would be no justifiable basis for Police Scotland to invest in this technology" and that the "live facial recognition software which is currently available to the police service is known to discriminate against females, and those from black, Asian and ethnic minority communities"[3].

We understand that technology is always advancing and that public sector bodies are increasingly adopting artificial intelligence (AI). This may be AI-powered computer software, systems or even biometric technologies such as live facial recognition (LFR). While we understand that the adoption of AI can help increase efficiency and save costs in the sector, there is a lack of proper governance, policies and accountability in place to ensure it minimises the ethical, legal, and social risks that AI poses.

It is in this view that CEMVO Scotland believes that any subsequent plans to roll out facial recognition and other biometric technologies further will carry real risks of exacerbating racialised inequalities already deeply entrenched in institutions and society.

Although this consultation is about exploring a new legal framework for law enforcement use of biometrics, facial recognition, and similar technologies, CEMVO Scotland's fundamental view is that the deployment of discriminatory software, such as facial recognition technologies (FRT), should be prohibited, considering the disproportionate interference with rights to privacy and other human rights. If plans for deployment were to go ahead, we have outlined our views in further detail below.

[1] BBC, 2025, 'Met Police facial recognition tech mistook me for wanted man' - BBC News
[2] Big Brother Watch, 2026, High Court to Hear Landmark Legal Challenge Against Police Live Facial Recognition — Big Brother Watch
[3] Justice Sub-Committee on Policing, 2020, Facial recognition: how policing in Scotland makes use of this technology | Scottish Parliament

Which technologies should the new framework apply to?

1. To what extent do you agree or disagree that a new legal framework should apply to all use of 'biometric technologies' by law enforcement organisations?

2. Do you think a new legal framework should apply to 'inferential' technology i.e. technology that analyses the body and its movements to infer information about the person, such as their emotions or actions?

3. Do you think a new legal framework should apply to technology that can identify a person's clothing or personal belongings, or things that they use (e.g. a vehicle)?

CEMVO Scotland believes that a new legal framework should be applied to all use of 'biometric technologies', especially given that there is a lack of legal basis for their deployment. We note that FRT can include different types: live facial recognition (LFR), retrospective facial recognition (RFR), and operator-initiated facial recognition (OIFR). Other biometric technologies can include inferential technology that can analyse body movements and infer data about a person. Such technologies are highly invasive and discriminatory in nature, and they pose a significant risk of violating people's human rights.

Under the European Convention of Human Rights (ECHR) and the Universal Declaration of Human Rights (UDHR), which are incorporated into the Human Rights Act 1998, the following rights are at risk of being interfered with: rights to freedom of expression, right to freedom of assembly and association, right to respect for private life, right to non-discrimination, and right to liberty and security. Meanwhile, the Public Sector Equality Duty requires public authorities in the UK to promote equality, eliminate discrimination, and ensure they consider how their policies affect people with protected characteristics.

Currently, the deployment of FRT is largely unregulated, as seen in England and Wales, and relies on inconsistent policies gathered from parts of equality, human rights and data protection laws.

It is also important to note that the level, scale, and kinds of negative human rights and race equality impacts would differ across various technologies mentioned above. When considering a new legal framework, it must weigh the nuances of different impacts so that it is adaptable and fluid, balancing the data protection, human rights and equality laws that it affects.

For example, deploying LFR involves indiscriminately scanning faces in public and people who are often unaware and have not given consent but are still subjected to LFR. This mass surveillance technology could mean breaching data protection rights, equality laws, and privacy rights on a larger scale.

In other instances, we know that OIFR can be used by police officers when they are directly engaging with members of the public. This involves taking a photo of the person's face and using a mobile app to compare it to what is held in their database, including their 'watchlist'. However, CEMVO Scotland is concerned that any further roll-out of OIFR will expand policing powers to the extent that it inevitably creates another dimension of systemic issues in stop and search. This is because evidence continues to show that Black people in parts of the UK are still five times more likely to be stopped by police than White British people per head of population[4]. The reality is that visible ethnic minority people are already disproportionately impacted by racial bias and profiling, and operating OIFR technology will mean undermining the foundations of race equality and human rights work that have been significantly achieved.

As demonstrated in these examples, we therefore recommend that further clarification be provided to explain the differing impacts that such technologies would cause to ensure the new legal framework is adaptable and balanced proportionately. We recommend using equality and human rights impact assessments in every possible process to effectively spotlight risks and gaps.

Which organisations should the new framework apply to?

5. Do you think a new legal framework should only apply to law enforcement organisations' use of facial recognition and similar technologies for a law enforcement purpose?

It is CEMVO Scotland's view that a new legal framework should apply to all sectors, including private, in order to uphold state obligations to promote, respect and fulfil our human rights.

FRTs are increasingly used by private companies in retail to scan members of the public, and much of the way they are used is intrusive and lacks the establishment of knowledge and consent. This highlights concerns that private companies are increasingly likely to interfere with our rights, which is ultimately unnecessary and disproportionate. Errors of FRTs at retail stores have also been reported. In 2024, Sara walked into Home Bargains to find that she was mistaken for a thief after being flagged by the facial recognition technology Facewatch[5]. Her bag was searched and she was asked to leave. This was incredibly distressing for Sara, and it is unacceptable that cases such as Sara's go unchecked. There is a risk of further unaccounted-for cases if the regulation does not extend to the private sector.

This will have serious social and legal consequences, and echoing fellow civil society organisations, it can create a 'chilling effect' that discourages people from exercising

[4] Institute of Race Relations, 2025, Criminal justice system statistics - Institute of Race Relations
[5] BBC, 2024, 'I was misidentified as shoplifter by facial recognition tech' - BBC News

their basic rights and being wrongly put on 'watchlists'[6]. Government and statutory bodies must take a leadership role in protecting people's human rights by ensuring that private sector companies are law-abiding and held to account.

When should law enforcement organisations be allowed to use these technologies?

6. When deciding on the new framework, the government will use the factors listed above to assess how law enforcement organisations' use of biometric technologies, such as facial recognition, interferes with the public's right to privacy. What other factors do you think are relevant to consider when assessing interference with privacy?

7. When designing the new framework, the government will also assess how police use of facial recognition and similar technologies interferes with other rights of the public. This includes things such as the right to freedom of expression and freedom of assembly. In addition to the factors listed above Question 6, which factors do you think are relevant to consider when assessing interference with other rights?

While we note that there is an acknowledgement of the risks of interference with privacy rights and what these factors might look like as outlined in the paper, we support other civil society organisations in calling for stronger safeguarding procedures to protect people's rights. For example, recent analysis (2025) of the police national database on retrospective facial recognition (RFR) technology found that Black women had significantly higher false positives at 9.9%, compared to 0.1% for white women[7]. This means Black females are much more likely to be misidentified than white females. This is incredibly alarming, which proves that much stricter safeguarding needs to be in place to prevent racial bias, discrimination and other human rights breaches.

Furthermore, to allow people to exercise their rights, notice of use of such technologies must be provided explicitly and with clear routes to redress if anything goes wrong.

For what purpose should law enforcement organisations be allowed to use these technologies?

8. Do you agree or disagree that 'seriousness' of harm should be a factor to decide how and when law enforcement organisations can acquire, retain, and use biometrics, facial recognition, and similar technology?

CEMVO Scotland firmly believes that if law enforcement organisations were to go ahead and use the above-mentioned biometrics, facial recognition and similar technologies,

[6] Big Brother Watch, 2023, Biometric-Britain.pdf
[7] The Guardian, 2025, Home Office admits facial recognition tech issue with black and Asian subjects | Facial recognition | The Guardian

they must do so in a way that is strictly necessary and proportionate. For that reason, the seriousness of harm should always be carefully considered in deciding how and when such technologies should be used. We believe that the threshold must be high for legitimisation of use, as it would otherwise be seriously disproportionate to low-level offences. Any decision to use must demonstrate the least possible interference with human rights, ensure transparency in use and implement strict accountability measures should there be a breach of rights or laws.

We recommend that the development of a new legal framework and regulations should be similar to that of the EU AI Act in that it broadly prohibits "real-time" biometric technologies such as LFR. Unless this is considered strictly necessary to be used for:

1) the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons
2) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack
3) the localisation or identification of a person suspected of having committed a criminal offence[8]

Who should decide when law enforcement organisations can use technologies like facial recognition?

10. The government believes that some uses of facial recognition and similar technologies require more senior authorisation and that this should be set out in the new legal framework. Do you agree? This could be different levels of authorisation within law enforcement organisations, or, in some circumstances, authorisation by a body independent of law enforcement organisations.

11. Are there circumstances where law enforcement organisations should seek permission from an independent oversight body to be able to acquire, retain, or use biometrics (e.g. use facial recognition technology)? This could include exceptional circumstances outside of the usual rules.

In a 2019 research study analysing the Met Police's LFR trials, Professor Fussey and Dr Murray found multiple failures in planning, methodology and operations. This included the failure to embed the principles of "necessity" and the establishment of consent. Operationally, this led to inconsistent verification processes and high levels of inaccuracies. All live trials were brought to an end, and it was recommended that

[8] 2024, Article 5: Prohibited AI Practices | EU Artificial Intelligence Act

fundamental compliance with human rights, appropriate governance and accountability are required to proceed.

Since then, however, such issues have continued in areas where law enforcement deploy FRTs, negatively impacting individuals while also being used on members of the public without clear notice and consent as mentioned above. CEMVO Scotland generally agrees that there should be senior authorisation of their use, but more importantly, we believe it should require an independent body, such as a judicial body, for authorisation and oversight. This would mean implementing a process where police explain clearly the rationale for use, the risks and how it will impact on rights, and demonstrate efforts to minimise interference.

The EU AI Act reflects such an approach, which we would recommend for similar adoption:[9]

"each use for the purposes of law enforcement of a 'real-time' remote biometric identification system in publicly accessible spaces shall be subject to a prior authorisation granted by a judicial authority or an independent administrative authority whose decision is binding of the Member State in which the use is to take place"

How should the new framework guard against bias and discrimination?

16. The government believes the new oversight body should help set specific rules for law enforcement organisations to follow, to guard against bias and discrimination when using technologies such as facial recognition, and check compliance with these rules. To what extent do you agree or disagree?

CEMVO Scotland strongly agrees that the oversight body should do everything they can to eradicate discrimination and guard against bias. We know that bias can never be truly eliminated, which is why we fundamentally disagree with FRTs or similar technologies in their further roll-out, given the disproportionate and unnecessary impacts they will have on visible ethnic minority and other marginalised people. It must be recognised that embedding race equality and human rights is crucial to underpin a new legal framework, and this needs to involve public scrutiny and debate. The new oversight body should support, guide, and ensure compliance with any specific rules set. Public and private sector organisations should be considered under the new oversight body to ensure stringent measures are taken, as exemplified by the EU AI Act.

To conclude, as a race equality organisation that continually engages with and supports public authorities, it is well known that the Public Sector Equality Duty (PSED) is flawed, often misunderstood and not complied with. If a new legal framework and oversight

[9] Article 5: Prohibited AI Practices | EU Artificial Intelligence Act

body are to be introduced for the use of biometric technologies, they need to be fit for purpose, robust, transparent and outcomes-focused so they do not merely become symbolic.