Scottish Biometrics Commissioner
Bridgeside House
99 McDonald Road
Edinburgh EH7 4NL

Home Office Consultations

Response sent by e-mail

Dear Home Office, 12 December 2025

Consultation on potential new blueprint and legal framework for England and Wales on law enforcement use of biometrics, facial recognition, and similar technologies

I write in response to the above consultation and in doing so seek to suggest a potential blueprint and legal framework for England and Wales on law enforcement use of biometric and forensic data, including facial recognition and similar technologies. For reasons of brevity and clarity, I wish to suggest some broad strategic principles for consideration rather than offering a view on specific lower order matters.

By way of introduction, I am the Scottish Biometrics Commissioner with responsibility in Scotland to ensure that biometric data and technologies are used lawfully, effectively and ethically by specified policing bodies in Scotland where such data is acquired, retained, used, or destroyed under domestic Scots law. The definition of what constitutes 'biometric data' in the Scottish Biometrics Commissioner Act 2020 covers both biometric and forensic use (DNA, fingerprints, images, and recordings etc) and is a broader definition than currently exists in England and Wales. As an independent officeholder in Scotland, I am appointed by the Monarch on the nomination of the Scottish Parliament. This means that the role is completely independent of Government and ensures no political interference. I am funded by, and report only to the Scottish Parliament thus strengthening democratic accountability.

I also maintain a Statutory Code of Practice covering biometric/forensic uses backed by legal powers to ensure compliance. The Scottish legal framework also involves a mechanism for data subjects to complain to my office in circumstances where a data subject is concerned that the Code may not be being complied with and I have associated investigatory powers, including the power to do anything necessary or expedient in the discharge of those functions. The model has been in place in Scotland since 2021 and works exceptionally well and is valued by the Parliament, Government, and policing bodies.

Against this introductory context, I now turn to offer some comments on the specific consultation questions:

Blueprint for change

Firstly, I agree that the Home Office are correct to explore opportunities to merge the existing functions of the Biometrics and Surveillance Camera Commissioner and the Forensic Science Regulator under a single umbrella body. This would of course necessitate legislative change but in my view, it is the correct strategic direction of travel.

Scottish Biometrics Commissioner
Bridgeside House
99 McDonald Road
Edinburgh EH7 4NL

In doing so, I would also encourage the Home Office to consider removing National Security Determinations (NSD's) from the new function and instead assign these to the Investigatory Powers Commissioner's Office (IPCO). Doing so would have several advantages. Firstly, it better preserves the covert/secret nature of the intelligence that often underpins NSD's by assigning responsibility to an organisation that already independently reviews applications from public authorities to use the most intrusive of powers and check that they are used in accordance with the law. Secondly, doing so would mean that the Commissioner in charge of the remodelled function would not require to be STRAP vetted by the UK Security Services making future selection and appointment processes possible without the involvement of covert agencies of the state thus strengthening democracy. Thirdly, it respects devolution and removes the ambiguity of a Commissioner for England and Wales having a statutory locus in Scotland and Northern Ireland on such matters given that Scotland now has a Biometrics Commissioner and Northern Ireland is legislating to do so. Fourthly, it better separates covert and overt uses of biometric data and technologies to more appropriate oversight bodies.

Importantly, the new oversight arrangements need to be 'meaningful,' and the existing arrangements leave strategic gaps, for example through the role of the Biometrics Commissioner not currently extending to the most widely used biometric in policing in the form of 'face.'

Enabling legal frameworks

Any proposal to merge the functions as previously described would require legislative change but could easily deliver on the stated policy objectives of amalgamation, upholding standards, investigating misuse, enforcing compliance, and affording public redress. I agree that the best way to exercise such independent oversight would be through the establishment of statutory codes of practice as currently exist for forensic science in England and Wales, but which do not currently exist for the police use of biometrics in England and Wales. Such codes of practice should also cater for the use of facial recognition and similar technologies.

Inferential technologies

Future oversight and codes of practice should cover inferential and behavioural biometrics to ensure that all such uses are lawful, effective, and ethical and that technologies and their outputs are scientifically valid and reliable. I would highlight the specific examples of the use of polygraph in England and Wales and using ANPR to profile driver behaviour as examples of the sort of 'Biometric Wild West' that ensues when the use of such technologies is not subject to 'meaningful' oversight.

Exclusions from Scope

England and Wales should revisit its definition of biometric data as it is not currently sufficiently wide in scope and is outdated focussing solely on DNA and fingerprints. In this regard, I would encourage the Home Office to look at the definition of biometric data in Section 34 of the Scottish Biometrics Commissioner Act 2020, and at Section 35 which allows that definition to be updated by the Scottish Minister's as new technologies or use cases emerge.

Scottish Biometrics Commissioner
Bridgeside House
99 McDonald Road
Edinburgh EH7 4NL

Against this context, technologies which track objects rather than individuals should be out of scope if such use is not being used to 'identify' individuals or profile their behaviour. If they do, then they should be within scope.

Advantages of Codes of Practice

Codes of Practice even if statutory can be amended and updated more quickly and therefore more frequently than creating or amending primary legislation. This means that Codes of Practice can keep up with rapid advances in technology whereas the law often cannot.

To whom should such Codes apply?

In the context of this consultation, I would recommend that relevant Codes of Practice for England and Wales should apply to all law enforcement bodies but should not extend to the retail sector.

The principles of such Codes

The guiding principles within such codes should provide a statutory and legally enforceable framework that also considers other legal obligations including criminal procedure law, human rights law, equalities legislation, UK GDPR and privacy considerations. Such Codes should be consulted on and should provide a means of enforcement and public redress. For example, the Scottish Code of Practice is designed around 12 principles and ethical considerations:

Figure 1: Principles of Scottish Code of Practice

The Authorising Environment

On overt surveillance technologies deployed in public places, there should be an agreed authorising environment in the same way as applies to covert surveillance by the police. In other words, good practice would be for any such deployments to be authorised by a senior police officer not below the rank of Superintendent.

Scottish Biometrics Commissioner
Bridgeside House
99 McDonald Road
Edinburgh EH7 4NL

Records of such authorisations and deployments should be kept for inspection by relevant oversight bodies.

Interoperability Frameworks
Any changes to the legislative framework for England and Wales should not allow law enforcement to have 'routine' access to the biometric databases of other branches of the UK State for example UK Passport images or UK driving licence images. Specifically, there should be no 'bulk washing' of passport or driving licence images against retrospective police facial recognition for low level or volume crime.

However, interoperability frameworks should be developed to cater for the 'specific' circumstances where such searching is permissible such as CT policing or as part of a strategic policing response to address violence against women and girls (VAWG) or Serious and Organised Crime Groups (SOCG).

This mirrors the needs-based approach that currently exists. For example, Police Officers can access a UK driving licence image from their PDA when dealing with a road policing matter and bespoke searching can be allowed for CT purposes.

I trust that these comments are of assistance.

Yours sincerely,

Brian Plastow

Dr Brian Plastow
Scottish Biometrics Commissioner