OFFICE OF THE BIOMETRICS AND SURVEILLANCE CAMERA COMMISSIONER

Home Office Consultation: A new legal framework for law enforcement use of biometrics, facial recognition and similar technologies

A response to the consultation by Professor William Webster, Biometrics and Surveillance Camera Commissioner

Summary

The Home Office's consultation on the proposed 'New legal framework for law enforcement use of biometrics, facial recognition and similar technologies' represents a **once-in-a-generation opportunity** to get a legal framework right and to design it in such a way that it enables the **appropriate** and **responsible** use of biometrics, facial recognition and other similar technologies in law enforcement and policing.

The new legal framework must include **a meaningful regulatory regime** which operationalises principles such as necessity, responsibility, proportionality, transparency, accountability and lawfulness. These principles should then structure and constrain law enforcement powers, enabling law enforcement to discharge their duty to protect the public while upholding and safeguarding fundamental human rights.

The framework must not be focussed on a narrow range of contemporary technologies, as technology types and capabilities evolve rapidly, instead the focus of the framework should be the **purpose** justifying the deployment of powers, the **principles** to be enshrined in the execution of these powers, and the **activities** associated with the use of these powers. Such an approach will ensure that the framework is **value driven**, rights respecting, future-proofed and can accommodate innovative emerging technologies.

The activities captured by the scope of the framework should be broader than (biometric) identification, and should cover, for example, the remote detection of criminal and undesirable behaviour, inferring criminal intent, and the identification and tracking of objects. Activities beyond those prescribed in the framework should be prohibited, unless subsequently amended following Parliamentary debate and scrutiny. The framework should therefore take **a legally codified restrictive approach**, which would mirror the approach taken in the Investigatory Powers Act 2016 and the Forensic Science Regulator Act 2021, in which carrying out specified activities is considered an offence unless the legal requirements for lawful use of powers are met and the parameters of the regulatory regime have been accommodated.

Core principles enshrined in the framework must include **a clear definition of 'seriousness of harm', 'intrusiveness' and 'law enforcement purposes'**, with **operational activities measured in terms of levels of risk and proportionality**. High risk activities should require pre-authorisation by an independent regulator. **Codes of practice** and standards for scientific evaluation, as well as **monitoring and audit practices,** would inform lawful use.

The new regulatory regime should **apply to police and other public and private organisations undertaking law enforcement activities**, including those pursuing **public safety** and **crime**

prevention. Restricting the scope of the framework to just law enforcement would exclude equally intrusive activities being carried out by other public and private sector organisations. To narrow the focus of the scope to just law enforcement also fails to take into account the **multitude of data sources that are used by law enforcement** but originate from other public service and commercial contexts.

The proposed new regulator **must be empowered and resourced appropriately** to deliver necessary meaningful oversight and must capture the **functions of audit, monitoring, inspection, compliance and reporting**, to ensure that the new regulatory regime is transparent, accountable, purposeful and efficient. The regulator should be **a 'one stop shop' single point of contact** for regulatory and oversight matters in this area. Built into its functions at the outset, should be an **independent advisory group**, and a requirement to **engage and advise the public** and to provide **foresight around technological development**. **Public reassurance** is critical to ensuring **confidence in policing and law enforcement** and to the deployment of emerging biometric surveillance technologies. A commitment to independent regulation comes with an expectation that certain uses of biometrics and similar technologies are disproportionate, publicly unpopular and **should not be permitted**. Whilst regulating the use of specified technologies the regulator will have a role to play in **ensuring innovation is appropriate** and aligned to the principles enshrined in the framework.

The framework must align to the **principles and values of our democratic system**. This includes minimising the risk of wrongful interference with **fundamental rights**, such as our rights to privacy, freedom of movement, freedom of association and safety, as well as not diminishing the presumption of innocence or restricting other freedoms. This is not a question of balancing rights to accommodate the use of contemporary technologies, rather the issue here is to make sure all rights are satisfied in the use of those technologies. This requires the framework to have a very clear definition of 'seriousness of harm' and 'justification for use' in order to determine if technological deployment is warranted. In circumstances where harm is disproportionate, the use of these technologies should not be allowed, with serious penalties and sanctions to act as a deterrent. The new regulatory body charged with regulatory oversight should be **independent,** have its **powers enshrined in legislation** and **report directly to Ministers and Parliament**.

1. Contextual Assumptions

1.1 The context for the proposal to regulate biometrics, facial recognition and other similar technologies incorporates a number of underlying assumptions:

- that the pace of technological evolution is rapid and unpredictable and that biometric and digital technologies are increasingly integrated into single systems and everyday life;
- that facial recognition technologies are diffusing quickly into a range of societal settings, including in policing, law enforcement and other public service and commercial contexts;
- that there is an expectation that law enforcement organisations should be able take advantage of emerging technologies to deliver their functions effectively and efficiently;

- that there is a recognition that – by definition – technologies like facial recognition compromise human rights and consequently there is an urgent need for them to be regulated carefully;
- that, in order to deploy such technologies law enforcement organisations need confidence about when, where and how they can be used;
- that there is a need to provide public reassurance and confidence that these technologies are used proportionally and lawfully;
- that relying on self-regulation and voluntary standards cannot be relied upon to safeguard human rights;
- that the technological starting point for the new framework is the use of sophisticated surveillance camera systems and that such systems go beyond simple data processing, because they embody the state surveillance of citizens;
- that the framework includes a legal definition of biometrics that incorporates aspects like faces, voices and irises; and
- that there is a recognition that the current regulatory landscape is overly complex and difficult to interpret, and that codifying principles, purposes, activities and technologies in a new framework will clarify the legal landscape.

2. A blueprint for the meaningful regulation and oversight of biometrics, live facial recognition and similar technologies in law enforcement

2.1 This response to the consultation offers up a **simple 'light touch' blueprint** to what the regulation of these technologies should look like. The focus here is on the principles and ideal components of such regulation and not their precise operational mechanisms. These can be determined in the fulness of time. The response is organised around two parts, firstly the principles and scope of the proposed legislative framework, and secondly the components and activities of the new regulatory body.

2.2 The key areas being consulted on, and which I respond to here, are:

- how biometrics should be defined and what technologies should be covered;
- which organisations should fall under the new legislative framework;
- what constitutes proportionate use; and
- what oversight, regulatory powers and accountability mechanisms are required.

3. The underpinning purpose of the new legislative framework

3.1 Over time, it has become evident that the use of sophisticated technologies, like facial recognition, offer the potential to make a significant contribution to the work of law enforcement, but at the same time they are intrusive and conflict directly with fundamental human rights. The proposed legislative framework must provide legal certainty around their use, and in doing so provide confidence for law enforcement and the public that their use is proportionate, justified and lawful. The starting point is the purpose of the framework, and not necessarily the technologies that are to be applied to it. In this respect**, the framework should be principles based and not technology led**. This is because primary legislation that

seeks to codify, define and control a specific technology will quickly find itself out-of-date and in need of revision. Detail about technology types and applications should be provided in codes of practice.

3.2 The primary legislation should set out the fundamental values, principles and purposes that can be universally applied to all technologies that fall within a generic definition of applicability ('biometric technologies'). This will ensure that the purpose of the legislation aligns to our societal democratic values. Such principles can represent a set of thresholds which determine if use is appropriate, and should include: proportionality, necessity, responsibility and validity, and placed alongside clear definitions and measures of 'seriousness of harm' and 'intrusiveness'. Determining whether these thresholds for use have been met will be dependent on the law enforcement (or other) purpose and the levels of risk, which in turn would structure the exercise of law enforcement powers and use. This would ensure the protection of the public, whilst upholding human rights. Primary legislation should set out core principles and purposes, whilst secondary legislation should set out a range of use cases and technology types, which can be revised periodically.

3.3 Contemporary surveillance technologies are opaque and difficult to comprehend, so to be effective the framework must be accessible and transparent. It needs to be clear to those deploying the technology and the public how it will be operationalised, how service providers will be held to account and the limits and scope of technological use. The existence of guardrails and safeguards needs to be explicit, with the regulator having powers to enforce them, and not just giving 'lip service' to a need to follow rules.

3.4 Public understanding and acceptance of these technologies does not just depend on the degree to which a technology 'works', but also on perceptions of injustice and levels of intrusion and fairness. Law enforcement uses of these technologies will always be seen by some as mass state surveillance, and some people will always feel unjustly targeted. There is often also an assumption that these technologies have been rigorously tested and used in line with specified purposes. If this is not the case, then the deployment of such technology risks the likelihood of harm and could create public resistance. Public acceptance may then be compromised, the technologies resisted, which in turn could compromise confidence in policing. With this in mind, the regulator and those organisations using the regulated technology have a role to play in ensuring the reliability of the technologies prior to adoption, as well as being an interface for public knowledge and perception. A key principle of the framework must therefore be the scientific reliability and validity of the proposed use of any such technology. Technologies that are unable to demonstrate a solid scientific evidence base should fall outside the scope of permissible activities under the framework. In this respect, the regulator has a role to play in ensuring the scientific validity of a proposed technology and in fostering appropriate innovation.

3.5 Contemporary thinking around the use of technologies that embody automated decision-making point to the need for a 'human in the loop', and that ultimately a human is accountable for any decision determined by an algorithm. Whilst there is always a risk that 'the human' becomes over reliant on, and unquestioning of, technology, it is important that the framework

states specifically that human operatives retain substantive oversight and are explicitly accountable for the use of a technology, especially where it involves levels of intrusiveness that compromise human rights. The framework must actively guard against the risk that policing activities are reduced to the automated execution of algorithmic outputs, ensuring that human judgment remains authoritative.

3.6 Definitions that will have to be clearly set out in legislation include: the 'principles' framing the legislation, including 'seriousness of harm' and 'intrusiveness', 'law enforcement purposes', including 'crime prevention', 'public safety' and 'safeguarding' purposes, 'biometric data' and other 'relevant data processes', 'activities' to be captured by the framework and the circumstances when the framework is applicable, which could be framed as 'relevant authorities' or the 'point of data capture'.

4. Scope of the legislative framework – Relevant technologies

4.1 The proposition in the consultation is that the framework will capture a range of biometric and inferential technologies used in law enforcement. Technologies under consideration are: [1] biometric technologies (e.g. fingerprints, DNA, facial images, voice, irises, and gait); [2] inferential technologies (e.g. emotions, behavioural and actions); and [3] object recognition (e.g. bags, vehicles (ANPR), clothing, hats and weapons). It is important to note that these technologies go beyond personal identification and include other purposes like tracking and predicting behaviour. The technology types being considered also go beyond biometrics and inferential technologies to include a range of digital data process and databases, including the use of Artificial Intelligence (AI).

4.2 What they all have in common is that they all rely on **the existence of surveillance cameras as the starting point for data capture**. With this in mind, it is important to ensure that the existing Surveillance Camera Code of Practice is retained, revised and closely aligned to the new framework. Arguably, the ownership of this code should transfer from the Home Secretary to the new regulator. It is also important to note that a narrow definition of different technologies may be counterproductive as emerging systems are likely to integrate different technologies. The framework needs to be specific enough to regulate existing technologies and flexible enough to accommodate those in development and not yet envisaged.

4.3 The framework must also take into account that these technologies can be used for intelligence gathering, investigations and for evidential purposes, that they may be used in real-time or retrospectively, and that they can also be used for covert surveillance. For these reasons the framework must be compatible with the Regulation of Investigatory Powers Act 2016 and the Forensic Science Regulator Act 2021. Beyond the technological and data artefacts of these technologies the framework needs to take a 'whole system' approach which considers, purpose, use, procurement, training, evaluation, public awareness and human interaction. Such an approach ensures such systems are not merely seen as data processes and instead recognise that they embody formal power and legal authority.

4.4 The speed of technological change and the need to safeguard human rights points to a principles and values based approach embedded in primary legislation, focussed on the purpose of systems, proposed activities and measures of risk, intrusiveness and harm, and which prioritises critical principles like proportionality, transparency, reliability, and integrity, and sets the threshold required for the lawful use of the proposed technologies. Requirements for permitted specific technology types can be enshrined in secondary legislation, which can be periodically reviewed and revised as technology and public opinion evolves.

4.5 The starting point for the scope of the framework in primary legislation should not be the definition of specific technologies but the principles, purposes and activities to be regulated (permitted and prohibited). Activities will need to be clearly defined and could include the capture, monitoring, identification, prediction, inference or other processing of biometric and behavioural data, or the automated processing of data relating to a person, by a law enforcement body or by any organisation for law enforcement, public safety or crime prevention purposes. Activities, technologies and data types need to be sufficiently broad, and not limited to biometric identification, in order to be relevant to systems that offer remote object identification and tracking, and the detection of anti-social behaviour.

4.6 The Investigatory Powers Act 2016 criminalises certain activities for specified agencies unless the Act's provisions are followed, with activities only permitted in certain circumstances. This creates a regime where there is permitted use of certain technologies where defined protocols are established and adhered to. Broadly speaking the new framework should follow this approach.

5. Scope of the framework – Relevant organisations

5.1 The proposition in the consultation is that the new legal framework should apply to law enforcement organisations for law enforcement and potentially safeguarding purposes. Such organisations would include police forces in England and Wales, British Transport Police and the National Crime Agency, and law enforcement activity by other public organisations such as the Environment Agency, HMRC and Border Force - but not other public services. This list of relevant organisations is far too narrow and does not take into account the operational reality of law enforcement's use of surveillance cameras and the data that they generate. In practice, many public space surveillance systems are operated by local authorities and other public organisations, with footage shared with the police either directly or on request. Very few systems are police owned, operated and controlled. Moreover, beyond public space systems the police increasingly have access to systems in the commercial sector, such as in retail, and even domestic systems, such as doorbells with surveillance camera capabilities.

5.2 The new regulatory regime should apply to police forces and other organisations for those activities undertaken for **law enforcement, public safety or crime prevention purposes, including safeguarding.** Restricting the new regime to just law enforcement would create a two-tier regulatory system (although the consultation document is silent on how non-law enforcement use of the technologies would be regulated), where other bodies may also be using similar biometric surveillance technologies yet are not subject to the same operational

rules, safeguards and oversight. This demarcation would also be problematic for the police use of data deriving from other public service and commercial systems and for creating legal clarity and simplification. It is also worth noting that local authorities have a legal duty to ensure community safety and that a number of commercial companies are using technologies, for example the use of facial recognition by retailers to deter and catch shoplifters. The closer integration of public services and commercial entities to deliver societal safety and the data sharing this facilitates suggests the importance of an inclusionary approach to the framework. The framework must therefore be broad enough to encompass all the activities associated with law enforcement, regardless of who undertakes them and where data originates. It should also be extended to activities associated with public safety that are designed to prevent or deter serious harm, and such safeguarding activity which is increasingly seen as part of wider law enforcement.

5.3 Restricting the framework to law enforcement organisations will create a perverse two-tier system where law enforcement use of these technologies is tightly regulated but use by other organisations is not, and this could lead to a scenario with a proliferation of potentially disproportionate and unreliable systems are introduced for a wide variety of purposes, including non-law enforcement purposes, but where the data they generate is expected to be used for law enforcement purposes. An alternative position would be to specify the organisations required to comply with the legal framework and require non law enforcement organisations to give the legal framework due regard. I would argue that this is insufficient given the potential for harm embodied in the technologies being considered.

6. Scope of the framework: Biometric data acquisition and other public records

6.1 The consultation proposes that the framework will allow law enforcement agencies to search and use other public records with these technologies and that these other public records could include driving licence and passport databases. Databases are integral to the operation of the technologies being considered by the framework and consequently should align to the principles and activities enshrined in the framework.

6.2 This would be consistent with a whole-system approach already mentioned and with the expectation that all technological components are competently regulated and scientifically reliable. In this regard, databases, if they are to be used for the activities specified in the framework, will need to comply with the principles of the framework and codes of practice that set out technical specifications for validity, reliability and proportionality. Access to data sets created by other public services and commercial organisations, for other purposes, will need to be strictly governed and controlled, and should be subject to the same principles and safeguards required by the framework.

6.3 Vital to any framework that seeks to oversee the use of facial recognition technology (amongst other things), will be the provision of a clear legal basis on which the police and other bodies captured by the framework can acquire, use and retain facial images. This is an important biometric identification tool, particularly as these images are used to populate the watchlists for facial recognition deployments, and their acquisition, retention and use have

been an ongoing concern for my predecessors. I am aware of ongoing work within policing looking at ways to manage the retention of custody images to ensure these are lawful, proportionate and consistently applied, which my office is fully engaged with, and see any legislation brought forward as a consequence of this consultation as the perfect time to put this retention on a clear statutory footing.

6.4 The Protection of Freedoms Act 2012 (section 29(6)) provides the meaning of 'surveillance camera systems' for the purpose of the Surveillance Camera Code of Practice. It specifically includes Closed Circuit Television (CCTV) and Automatic Number Plate Recognition (ANPR) systems, as well as other systems for recording or viewing visual images for surveillance purposes, and systems for storing, receiving, transmitting, processing or checking the images or information obtained from these. Cameras for the enforcement of speeding offences are excluded from the requirements of the code and, while I do not suggest that they should be brought into the remit of the new regulator, this consultation provides the ideal opportunity to review the definition of surveillance camera systems and update where appropriate: while we all understand what CCTV is, to suggest many of the systems operating today remain 'closed circuits' is a little disingenuous. Furthermore, technology has advanced apace since the last iteration of the code, allowing capabilities like facial recognition technology to be added to, for example, ANPR and unmanned aerial vehicles (drones), and clearly needs to fall within the remit of the new regulator.

6.5 The framework will need to incorporate guidance to facilitate international data transfer and storage of biometrics that align to existing practices for DNA and fingerprints, as well as international regulations like GDPR.

7. Scope of the framework: Deployment

7.1 The consultation proposes that the framework will set limits that appropriately balance the level of interference caused by facial recognition and similar technologies against the seriousness of harm the use is intended to prevent or detect. The legal framework must set out the very strict circumstances under which these technologies can be used. Their intrusiveness and impact on human rights needs to be recognised at the outset, so that the use of these technologies is appropriate and proportionate and in line with human rights law. Consequently, the use of intrusive technologies should only be used for very serious offences and not minor infringements - this is essential if public support is to be maintained.

7.2 Within primary legislation the framework should focus on the principles, purposes and activities to be conducted in a way that they are universally applicable to all organisations required to adhere to the framework. Such an approach would not be technology-led and would be future-proofed to accommodate technological change. This framework should present a codified restrictive position whereby conducting a specified activity is an offence unless strict criteria set out in the legislation and relevant codes of practice are met, including the organisations using it. Sitting under the legislation should be secondary legislation in the form of a statutory code or codes of practice setting out the rules surrounding the development and deployment of a technology. Any code or code of practice should be owned

and updated by a statutory independent regulator. Code(s) could include a list and definition of permissible activities and technologies, and should be periodically reviewed and updated. This could then take account of changes in technological capability, the scientific reliability of technologies, and changing public attitudes towards certain technologies.

7.3 The independent regulatory body should play an oversight role in determining the permissibility of technology 'types' and not individual systems and should be a requirement of the regulator in primary legislation. This would include an assessment using criteria specified in legislation and which could include activity, purpose, seriousness of harm and intrusiveness (all of which are defined in primary legislation), and which could be used to determine levels of risk and harm, and consequently the subsequent regulatory requirements for use. A low-risk activity, with low levels of personal intrusion, may require an organisation (operator) to adhere to the regulator's code of practice and be subject to appropriate audit. A medium-risk activity, with more intrusion, may require the organisation to notify the regulator of its scientific validity and evaluation, as well adhere to any codes of practice and be subject to appropriate audit. For a high-risk activity with high levels of intrusion, the regulator should be expected to ensure that the technology has been properly evaluated and that its compliance with the framework is evidenced prior to and during use.

8. A new statutory regulatory oversight body

8.1 The consultation proposes a new regulatory body with statutory status to be formed by merging and expanding the roles and functions of the Forensic Science Regulator and the Biometrics and Surveillance Camera Commissioner: *"We envisage giving this body the necessary powers to provide assurance that law enforcement use of biometric technologies is legal, responsible, and necessary. These powers could include setting standards to assure scientific validity, issuing codes of practice and investigating instances where a technology has been misused, hacked or accessed without authorisation".*

8.2 The Forensic Science Regulator and the Biometrics and Surveillance Camera Commissioner have legally distinct defined functions with overlap around the evidential quality of surveillance camera footage. Their powers are derived from the Forensic Science Regulator Act 2021 and Protection of Freedoms Act 2012 respectively. It is crucial that these functions are protected and integrated into the framework and regulatory body. Their existing powers of inspection, authorisation, audit and reporting should be expanded to meet the needs of the new framework.

8.3 The success of the framework is dependent on effective oversight by an independent regulatory body with adequate powers and resources to conduct its business and particularly to enable appropriate use of technology and to identify and sanction unlawful activities. Voluntary self-regulation, given the potential for individual and societal harm, will not be sufficient to ensure compliance with standards. The regulator must make compliance mandatory, offer proactive oversight with an inspection and compliance regime, and be able to enact swift remedies where compliance is not evident.

8.4 The effectiveness of the new oversight body will be partly determined by the availability of resources to carry out its functions, this is particularly relevant given the potential to greatly increase the scope of its activities. While it is not appropriate to get into a discussion about budgets here, one issue of great importance to the new regulator's structure is resilience in the role of the regulator themselves. This is particularly pertinent for the biometrics casework currently undertaken by my office (under s63G of the Police and Criminal Evidence Act 1984, and National Security Determinations), responsibility for which would transfer to the new oversight body. The Protection of Freedoms Act 2012 is clear that only the Biometrics Commissioner can consider such applications. Consequently, following a significant period of time during which there was no Biometrics Commissioner, a considerable backlog of applications awaiting consideration by the Commissioner has built up. In order to mitigate the risk of this happening again, through a gap in appointment or extended absence for whatever reason, the legislation must allow others to carry out the functions of the regulator. There is precedent for this elsewhere, for example the role of the Investigatory Powers Commissioner (with a deputy Investigatory Powers Commissioner and Judicial Commissioners to which the Commissioner may delegate functions), and the Information Commissioner also has powers to delegate functions to their deputies. Such resilience will ensure continued, effective oversight, with timely decisions on applications made, and unnecessary and disproportionate biometric retention avoided.

8.5 An independent regulator will ensure a standardised coordinated approach across England and Wales and will ensure that the organisations required to adhere to the framework are not using similar technologies in different ways. This will also give these organisations a clear mandate to use technology when it meets the requirements of the framework. The new regulator should be legitimate, empowered, transparent, proportionate, consistent, accountable, expert, purposeful and specific. The new regulator should, in order to provide meaningful oversight:

- be independent of government, with purpose and powers enshrined in primary legislation;
- have regulatory primacy in relation to law enforcement, crime prevention, public safety and safeguarding purposes;
- operate under the principles of the new legislative framework;
- be a single point of contact, 'a one stop shop', for those using these technologies and the public;
- be an enabler to encourage the appropriate proportionate use of specified technologies; and
- be to be appropriately resourced to carry out its legislative functions.

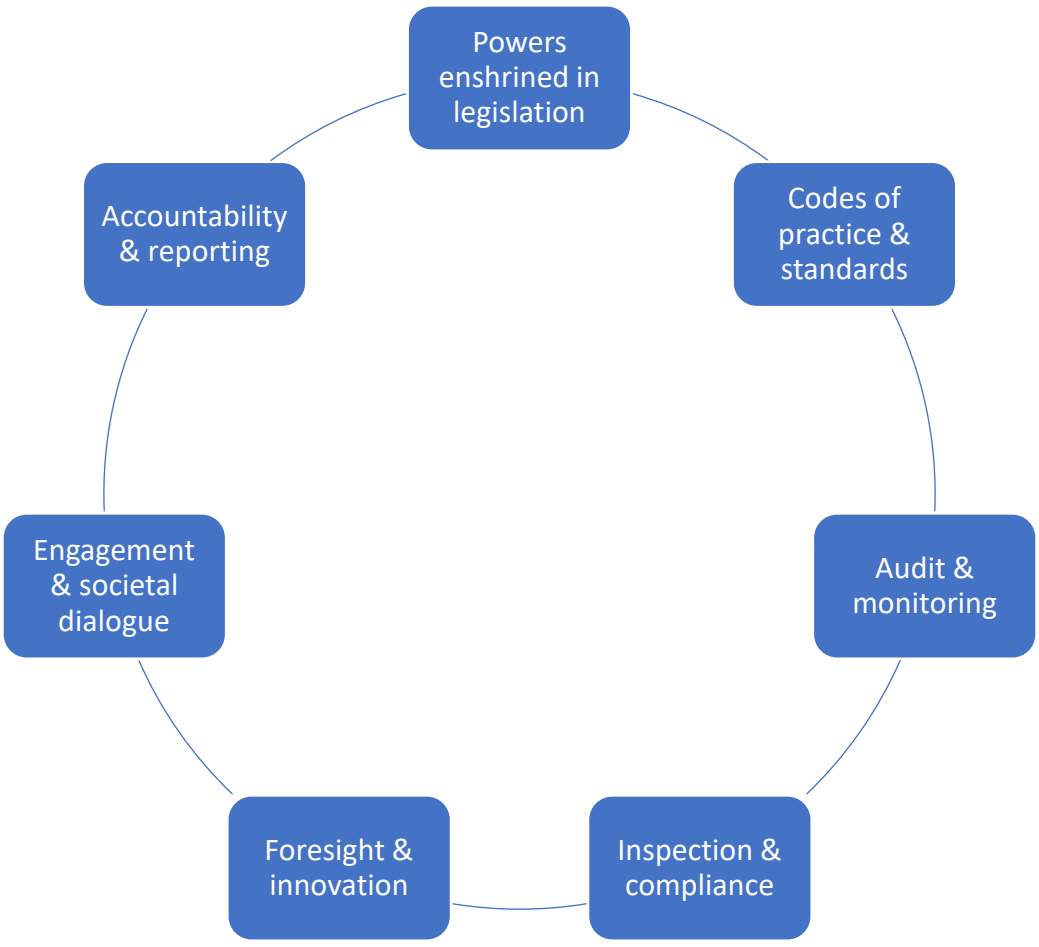
8.6 The consultation asks what functions this body should have, and suggests that they could include: publishing codes of practice, undertaking investigations, requesting information, issuing compliance notices, seeking injunctions, making public declarations, receiving complaints, publishing reports, and setting standards, etc. My response to this aspect of the consultation is organised around the core functions of a new regulatory body. The level of detail presented here does not necessarily cover the precise operational mechanisms

required, but identifies those areas where mechanisms are required and where further thought and consideration is required.

8.7 Figure 1. illustrates the functional components an effective oversight regulatory regime. This is not an exhaustive list of components, nor are they mutually exclusive.

- purpose, type and powers (establish legal authority and scope (discussed above));
- codes of practice and standards (to establish necessary specifications);
- audit (to record use);
- inspection and compliance (to facilitate appropriate use and instruct remedies);
- accountability and reporting (to establish necessary oversight, answerability and transparency);
- engagement and societal dialogue (to aid understanding and co-produce outcomes]; and
- foresight and Innovation (for forward planning and to facilitate responsible development).

Figure 1. Functional components of new oversight body



8.8 Under the new framework, the regulator should be expected to:

- produce code(s) of practice for low, medium and high-risk activities and technologies, incorporating existing legal frameworks and requirements;
- conduct or commission scientific evaluations of specific applications and possibly certify applications of high-risk use-cases;
- set standards for user evaluations, including assessments of validity, effectiveness and proportionality;
- have a role in determining when a new code of practice is required;
- provide oversight of provisions in Part V PACE and other relevant legislation relating to the acquisition, retention and use of biometrics and other specified data processes;
- fulfil statutory casework functions relating to s.63G PACE and National Security Determinations;
- set, oversee and enforce scientific standards;
- set use protocols covering expectations about how the technology is deployed;
- set standards and protocols for training and accreditation for users;
- conduct periodic monitoring and inspection of systems and users, and audit compliance with codes of practice and standards;
- issue enforcement compliance orders, make public declarations about non-compliance and prosecute if necessary;
- appoint and consult an independent advisory panel (or expert advisory group) for technical advice and to highlight future developments;
- undertake public engagement, potentially as part of the independent advisory panel, to co-produce regulatory outcomes;
- advise on when a new biometric and associated activity should be added to the framework;
- have a clearly defined relationship with other relevant regulators and oversight bodies as required, including the ICO, EHRC, IOPC, IPCO and HMICFRS; and
- report activity and levels of compliance annually to Ministers and Parliament.

9. Codes of practice and standards

9.1 The regulatory body should be expected to set out clear policy, procedures and standards (codes of practice) for those organisations required to adhere to the framework. These standards should cover 'fit for purpose', governance and technical specifications, and should be closely aligned to the principles set out in primary legislation. A statutory code of practice which is technology generic should set out the overarching principles, purposes and activities permitted by the regulator. This should be non-technology specific, principles-based and should set out proportionality tests and prescribed activities. This will constitute a national standard for England and Wales.

9.2 Sitting under this principal code should be a series of technology 'type' codes or standards setting out the protocols and standards required for the development and deployments of different 'types' of technology, and which carry the same legal weight as the primary code of practice. These will cover: purpose, ethics, technical specifications, use protocols,

procurement, training, risk analysis, performance measurement, evaluation mechanisms, guardrails, and due regard and compliance with other relevant legislation. Compliance with these codes will be mandatory, and they will be regularly reviewed by the regulator in conjunction with stakeholders and experts. Compliance with these codes will provide a degree of legal certainty, would ensure regulatory coherence, and thereby simplify the regulatory landscape. It would be expected that these codes to incorporate and evolve alongside existing international standards, such as those produced by the BSIA (British Security Industry Association) and other regulatory instruments, such as Data Protection Impact Assessments.

9.3 Robust codes of practice should include the factors required to operationalise the key principles of the framework, including reasonableness, proportionality and assessment of harm. They should include, but are not limited to:

- specific measures to ensure other rights are accounted for, in particular: Article 8 (privacy), Article 10 (freedom of expression) and Article 6 (fair trial) concerns, as well as Police and Criminal Evidence Act (PACE) issues around stop and search and the collection, use and retention of biometric material;
- methods to ensure scientific validity and approved evaluations;
- requirements for human authorisation mechanisms around automated decision-making;
- rules requiring documented justification for use, and incorporating Data Protection Impact Assessments and Equality Impact Assessments;
- rules governing the creation and use of databases, including 'watchlists' and auditable data acquisition, retention, use and destruction methods;
- rules governing the independent periodic testing of algorithms, as well as evaluating their operational performance;
- rules setting out thresholds for use, levels of authorisation required and the exceptional instances when the agreement of the oversight body is required;
- rules governing the quality of biometric and data processes required to ensure evidential quality material;
- rules around engagement of other relevant regulators, the public and stakeholders; and
- rules governing the ethical procurement of systems and operational training protocols.

10. Monitoring and evaluation

10.1 A key function of the new regulator will be to provide users of in-scope technology with the codes and guidance that set rules and expectations around the ongoing monitoring and evaluation of any proposed and used technologies. This should include independent evaluations prior to and during use. These evaluations must include post deployment real-world operational assessments. The regulator should have oversight of these evaluations and could conduct these evaluations itself or oversee their commission. All evaluations must be independent, scientifically robust, valid and grounded in operational reality. In this respect, the regulator must possess the tools and expertise to evaluate technologies and to operate a process for approving prescribed technologies and use cases. The regulator should also play a role in making sure that evaluations are accessible and clearly communicated to stakeholders and the public prior to deployment. This is especially important where complicated statistics

are used and where technological outcomes could be used evidentially. Operational thresholds and false positives/negatives must be carefully monitored and audited.

10.2 Areas to be incorporated within evaluations should include: the evidence base of initial knowledge and operational requirements, the identification and collection of real-world policing data that can be used as a test bed for the evaluation of technologies, an assessment of the impact of natural environmental factors such as weather and lighting as how this impacts outcomes (for facial recognition for example), an exploration of which algorithm outcomes (e.g., false positives) arise when different thresholds are set, and qualitative assessments of the technology to compliment statistical analysis.

10.3 Undertaking robust evaluations can be time consuming and expensive and there is a risk that independent testing is substituted by supplier-led assessments. An independent regulator would mitigate this risk by having a standard national process. If the regulator was not resourced to conduct these evaluations itself, then a credible alternative would be for the regulator to set up standards for and licence evaluation to trusted independent third parties.

11. Audit, inspection and compliance

11.1 The new regulatory body must have powers of audit, inspection and compliance - to ensure compliance with codes and standards set by the regulator. The regulator should be responsible for the periodic audit of systems with these audits organised around the principles and activities set out in the legal framework. Annual summaries of the audits should be reported directly to Ministers and Parliament (see below). Auditing can take a variety of forms and may include self-audit and self-reporting to demonstrate compliance, with the regulator having the power for periodic sampling to check accuracy. Here there would be a requirement for users to comply with the audit process, with non- or partial engagement penalised.

11.2 The auditing process must include the power of inspection, which would include site visits and a requirement for the engagement of responsible office holders. These site visits could replicate the existing site visits conducted by my office to oversee biometrics retention practices in police forces and use of open space surveillance technologies in line with the Surveillance Camera Code of Practice. They could cover, for example, checks to confirm the inclusion, retention and deletion of images on a watchlist are being adhered to and authorised by an appropriate officer, which would be set out in the new framework, or instances where use poses risk to criminal investigations or proceedings. These inspections should be conducted by the regulator, although they could be organised to coincide with inspections carried out by His Majesty's Inspectorate of Constabulary and Fire and Rescue Services.

11.3 In addition to powers of audit and inspection the new regulator must have compliance powers so that activities and technologies are regulated effectively. These compliance powers could take a variety of forms with different levels of severity. The regulator could issue a compliance notice on a user as a form of enforcement action, which could require the law enforcement body to take specific actions to remedy non-compliance. This could specify necessary changes required in order to conform with the principles and activities enshrined in

the framework. For more serious non-compliance the regulator could issue an instruction to stop using the technology where it poses significant potential harm to the public. This legally enforceable power could ultimately be achieved by seeking an injunction against the organisation(s) deploying the technology. There could also be an expectation that the regulator will make Parliament, Ministers and the public aware of any non-compliance, for example through inclusion of infractions within the annual report to Ministers.

12. Accountability and reporting

12.1 The regulator's core functions should be set out in statute. This is important for independence, transparency and accountability. The regulator should report directly to Parliament, through an annual report to the Home Secretary, similar to the requirements of my current roles. This report should include an overview of annual activities and compliance with codes, standards and inspections. The regulator should also be able to provide ad hoc advice and reports to Ministers, and for these reports to be laid in Parliament. The functions and activities of the regulator must also be publicly accessible through the Internet, with dedicated web pages for the regulator.

12.2 The regulator should also include an anonymous reporting function for biometrics and surveillance camera experts (and potentially members of the public) to report concerns about deployment and compliance with codes. This would mirror the 'anonymous reporting line' set up by the Forensic Science Regulator.

13. Public engagement and societal dialogue

13.1 Meaningful public engagement should be a core component of the regulatory oversight body from the outset. This would play a key role in generating broader societal understandings of the technologies, their purposes and consequences, and provide reassurance that technologies are socially acceptable. Communities directly impacted by the use of these technologies should be actively engaged by the regulator and have a direct input into decision-making concerning their development and use. Engagement that is inclusive, accessible and ongoing is required to ensure informed, balanced and legitimate outcomes.

13.2 There are a variety of public engagement mechanisms that could be utilised to achieve this functionality. Ideally, this would be in the form of genuine representation and be more substantial than what can be achieved through general consultation. An ideal here would be to create a regulatory participatory oversight committee (or Independent Advisory Panel) which has representation of different relevant community groups and stakeholders. This would ensure that the process of technological adoption has integrity and gives participants a mandate through which they can express their views and shape practice. Giving participants an advisory capacity safeguards against technological creep and unexpected deployments.

13.3 It is important that the panel meets regularly and considers all aspects of technological development. This would allow for the co-production of problem definition, solution recognition and decision-making that is shared and transparent. Mechanisms for engagement

should be designed to ensure the public and communities have genuine influence, with clear routes to shaping decisions, and engaging in governance arrangements. The regulator should encourage inclusive and representative participation and involve communities most likely to be affected by technology, including marginalised and under-represented groups.

13.4 The regulator should provide information directly to the public via a dedicated website, which would contribute to the societal awareness of biometric surveillance.

13.5 The regulator should work with the Independent Office for Police Conduct (IOPC) to handle complaints about misconduct in the use of biometrics and related technologies.

14. Foresight and innovation

14.1 The regulatory body should incorporate a foresight function to consider emerging gaps in oversight as technology and practice evolves. A foresight function could be formally integrated into an Expert Advisory Group, which could be part of, or separate from, the Independent Advisory Panel mentioned above. A foresight function could be used to influence technological development and utilised to ensure that innovation embodies the principles and values enshrined in the framework. Contemporary oversight bodies typically run innovation 'labs' and 'sandpits' to facilitate innovation and good use cases. They are a feature of the regulatory landscape and facilitate research, responsible innovation and development, and could provide a 'safe space' for organisations to initiate a trial/pilot of a new initiative. Whilst primarily for law enforcement initiatives they could involve a range of partner bodies. In practice, these labs facilitate knowledge sharing, best practice, responsible and ethical use, and provide advice on legal requirements. This would also mitigate the inherent risks of software and tech developer making direct approaches to law enforcement organisations, offering new technologies to seniors at reduced cost, and those technologies being deployed without clear understanding of their capabilities and risks.

14.2 Delivering labs and sandpits can be expensive and burdensome and there are a variety already in existence. The proposition here is not necessarily to set up a dedicated new facility, but that initiatives captured by the framework are exposed to a lab environment as part of their development. This can be achieved via a fast-stream set of protocols to ensure initiatives have been fully considered before being trialled. Protocols would cover purpose, proportionality, intrusiveness, risks, ethics, data protection, guardrails, duration and evaluation and would align to the principles enshrined in the new framework. The regulator would not be authorising initiatives or stifling innovation, rather it would be fostering appropriate innovation. Existing labs could be used, with oversight from the regulator, and with the expectation that the protocols established by the regulator are adhered to. This process could be certified. Existing labs could include the AI GrowthLab, the National Police Chief's Councils' Lab Police.AI or labs operating in the academic or private sector subject to a commercial arrangement.

Professor William Webster, Biometrics and Surveillance Camera Commissioner
12 February 2026