Information Commissioner's response to Home Office Consultation on a new legal framework for law enforcement use of biometrics, facial recognition and similar technologies

Summary

The Information Commissioner's Office (ICO) supports the responsible use of facial recognition technology (FRT) and other biometric technologies by law enforcement to prevent and detect crime. Such tools can play an important role in public safety, provided their deployment is lawful, proportionate, transparent, and supported by effective safeguards. The government's ambition to provide greater clarity and certainty in this area is welcome.

Data protection law must remain central to the governance of biometric technologies. It provides crucial protections, requiring organisations to balance law enforcement objectives with peoples' rights and freedoms. These laws are technology-neutral and designed to interact with other statutory frameworks. Any new regime must build on these foundations rather than replace them.

We recognise the value of additional legal specificity for law enforcement use of biometric tools. Clearer rules and consistent safeguards can support public confidence and improve regulatory oversight. Such clarity is especially important because law enforcement bodies use these technologies in varied ways, including procuring third-party systems, conducting retrospective searches using non-law enforcement databases, and collaborating with other public bodies.

Ensuring regulatory coherence and clarity will be critical. To ensure compatibility with data protection requirements and to mitigate the risk of divergent approaches and interpretation by oversight bodies, it will be important to incorporate statutory consultation requirements, including for the new oversight body, and develop memoranda of understanding

(MoUs) to underpin and support effective ways of working and collaboration.

Our role and mission

We have responsibility for promoting and enforcing the:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018 (DPA), this includes part 3 which governs the processing of personal data for law enforcement purposes;
- Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations 2004 (EIR); and
- Privacy and Electronic Communications Regulations 2003 (PECR).

We are independent from the government and uphold information rights in the public interest, promoting openness by public bodies and people's data privacy. We do this by providing guidance to people and organisations, solving problems where we can, and taking appropriate action where the law is broken.

The role of data protection law and the ICO in regulating biometrics, facial recognition and similar technologies

Data protection law applies to all processing of personal information. Therefore, any technology which processes personal information is subject to data protection rules. If law enforcement agencies use FRT or biometric technologies to identify living people, this use is governed by data protection law and falls within our regulatory remit.

Data protection law is designed to be technology-neutral. It provides a general framework of principles under which legitimate aims (eg public safety and law enforcement purposes) can be balanced against the protection of people's rights and freedoms. It recognises the relevance of other laws and is designed to interact with them.

Data protection law provides important protections and rights, including:

- a security principle which ensures people's information is protected from unauthorised access and loss;
- individual rights like access to personal information; and
- rights of redress.

We have a range of statutory functions, principally set out in articles 57 and 58 UK GDPR, and section 116 and schedule 13 of the DPA. These allow us to provide wide-ranging oversight of law enforcement processing of personal information, including through:

- advice;
- guidance;
- dealing with complaints from the public; and
- where necessary, issuing enforcement notices requiring rectification of non-compliant data protection practices and monetary penalties.

A full list of these functions is set out in annex two.

Our activity

Our research to understand the public's views and experiences of biometrics technologies shows that the majority agree that these technologies can bring significant benefits. But they remain concerned about the risks that these technologies pose if not used responsibly and with proper governance and safeguards in place. We have a longstanding history of work on the use of personal information in law enforcement, including the use of AI, biometric recognition and FRT. Our oversight and engagement has played a crucial role in ensuring the governance and safeguards that the public expect are in place.

Our focus on law enforcement includes significant projects that have shaped understanding and practice, such as:

- In 2019 we published an Opinion on the use of live facial recognition (LFR) technology by law enforcement. This built on our investigation into trials of this technology by South Wales Police and the Metropolitan Police Service.
- In 2022, we issued an enforcement notice against Clearview AI, an American facial recognition company that scraped billions of facial images from the internet without consent.
- We continue to update our guidance, providing LFR case studies and LFR practical checklists addressing FRT use by law enforcement organisations. We also provided input to the Scottish Biometrics code of practice and the Surveillance camera code of practice.
- As part of our AI and biometrics strategy, published in 2025, we have included a focus on the use of facial recognition technology in law enforcement. We are auditing police forces using FRT and will be publishing our findings as we did in our audit report of South Wales police and Gwent police.

This activity sits alongside our broader work on AI and biometrics, including the other work strands in our strategy, our insight and technology reports and our biometric data guidance.

Our comments on proposed new framework

Our views on the specific questions posed in the consultation are set out in annex one. However, we've summarised below our overarching observations about the proposed framework, and particularly the interaction with the data protection legislation and our regulatory remit moving forward.

Ensuring clear regulatory requirements

The consultation proposes introducing a new legislative framework and regulator to oversee the use of biometrics, facial recognition and similar technologies used by law enforcement agencies.

We recognise the benefits that greater legal specificity around law enforcement use of biometric technologies, including FRT, could bring to the police and the public. Clearly defined, objective requirements and safeguards in legislation could help ensure the consistent use of these technologies.

It is important that this specificity builds on, rather than seeks to replace, existing data protection legislation. Data protection legislation already:

- sets out key requirements to ensure appropriate oversight and governance;
- affords important information rights and provides routes for managing individual complaints and reporting personal data breaches;
- imposes core considerations to guide use, including that the processing is:
  - strictly necessary for the law enforcement purposes;
  - proportionate and effective, including that there is no less intrusive means of achieving the same outcome;
  - transparent;
  - accurate, including that appropriate steps have been taken to identify and eliminate bias; and
  - secure, with technical and organisational measures in place to protect the information.

Any new requirements need to be clear on how they interact with existing data protection law. Without this, we believe there is a risk that creating a new legislative framework and regulator could overlap or duplicate responsibilities and requirements or result in different regulatory bodies taking different approaches to key principles.

In our view, the most effective way of mitigating this risk is to set out in the legislation a greater level of specificity on the use of FRT and similar technologies in law enforcement. This would ensure that all relevant regulators are able to draw on clear, consistent and specific provisions for

when and how these technologies should be used. Any such specificity in the legislation could then be reflected in the way in which data protection legislation is applied, including decisions about fairness, lawfulness and compatibility.

If the desired specificity is to be achieved instead through statutory codes of practice that reflect and build on a range of regulatory requirements, including data protection law, it is imperative that the ICO is a statutory consultee. It would be preferable that responsibility for developing such codes rests with the Secretary of State, rather than the new oversight body. We also believe that Parliamentary approval should be required. This is so that those responsible for the relevant policy decisions approve any regulatory duties or responsibilities that are in tension and need to be reconciled. This approach is reflected in the Protection of Freedoms Act 2012 where the Secretary of State was required to consult the Commissioner about the development of the surveillance camera code and must also consult him about any alterations or replacement code. As noted above, the Commissioner provided substantial input to the most recent version of the surveillance camera code to ensure data protection requirements were considered.

We would expect any new framework content (or alternatively the content of any codes of practice) to be fully and robustly tested against data protection requirements to ensure it is compatible with data protection requirements before being finalised. For example, if the new framework provides that the use of FRT is permissible in a specified set of circumstances, we would expect:

- the use and set of circumstances to have been properly tested against the concepts of 'necessity' or 'strict necessity', 'fairness' and 'compatibility of purpose' in data protection legislation; and
- whether there are less intrusive means of reasonably achieving the same purpose to have been considered.

The new framework should include clear mechanisms that set out how new technologies or additional capabilities should be independently tested, so it is clear how they perform. The new oversight body could determine more prescriptive technical standards and independent testing requirements to provide additional safeguards and a greater degree of proactive scrutiny. Consultation with existing regulators, including us, would be important to ensure compatibility, interoperability and coherence.

Scope considerations

In our view, the new framework will only meet the aim of increasing clarity and confidence for both police and the public if it provides a

greater degree of specificity about particular technologies than that already provided by the existing, principles based, data protection framework.

We suggest that for maximum benefit, any new framework should aim to cover as many relevant law enforcement use cases and technologies as possible. Also that it includes appropriate public safety use cases, such as missing persons.

When developing the framework, it is important to consider the range of ways in which technology is currently used for law enforcement purposes and the range of bodies involved in those uses. This is alongside considerations about where legal obligations and liabilities under it should fall, and the coherence with the existing complementary data protection framework. The range of bodies involved in use cases include, for example:

- Law enforcement organisations developing and operating their own biometric and FRT systems, based on data they hold and used solely for law enforcement purposes.
- Law enforcement organisations procuring third-party systems where the law enforcement organisations may or may not themselves hold the relevant data, or some or all of the operation and associated processing is carried out by third-party public or private bodies, or both. This includes scenarios where law enforcement organisations use other public sector databases for retrospective facial recognition purposes.
- Law enforcement organisations working in partnership with other organisations. For example, local authorities, where the law enforcement body does not own or operate the biometric or FRT technologies but is able to use the data generated for investigative or evidential purposes, or both.

It will be important that there is clarity about how and when any new framework, and the scope of any new oversight body, applies to the kinds of use cases, and the range of bodies, set out above. This will be particularly important when thinking about how any new legislative requirements interact with existing data protection requirements. This is because these apply to all organisations and require clearly defined lines of accountability for compliance.

Similarly, significant work would be required if there is an appetite to expand the approach taken to law enforcement oversight to non-law enforcement organisations. This is either where that processing may generate information of interest or relevance to law enforcement, or

where information is processed entirely for non-law enforcement purposes. This would include any decision to pursue the option of a 'have regard to' approach as noted in the consultation. Further public policy analysis, wider consultation and more detailed parliamentary debate are necessary before any such decisions or additional changes to the legislative framework are taken forward. This includes greater clarity about how such arrangements would be overseen and enforced.

Regulatory oversight

The consultation proposes a 'one-stop shop' regulator encompassing and building on the Biometric and Surveillance Camera Commissioner (BSCC) and Forensic Science Regulator (FSR). It gives this new body an oversight role for FRT and potentially other biometric technologies used in law enforcement.

We assume that this does not indicate an intention to remove the role of the ICO in overseeing the processing of personal information by law enforcement organisations as set out in part 3 of the DPA and recently amended by the Data (Use and Access) Act (DUAA).

In principle, we have no objection to the proposal to merge the roles of the BSCC and the FSR. However, it will be important to consider how this interacts with our role should the new body be given:

- additional powers;
- the ability to set out regulatory requirements in codes of practice; and
- duties to ensure that law enforcement organisations are using FRT and biometric technologies responsibly.

We are keen to ensure there are no contradictions between the expectations of law enforcement organisations under data protection law and any requirements set out by the new body. It also needs to be clear how and when each body would exercise its powers.

There is a risk that creating a new regulator introduces the potential for inconsistent or contradictory regulatory decisions being made by the different oversight bodies that will continue to have jurisdiction.

It is notable that codes of practice are not usually directly enforceable. Instead, oversight bodies exercise their powers about the underlying legislation that the codes are built on. Should the new framework encompass codes of practice that address requirements under different legislation, including data protection legislation, it will be even more important that enforcement and oversight responsibilities are clear.

It will also be important to ensure clarity about how people can exercise their rights and seek redress when things go wrong. Memoranda of understanding (MoUs) and statutory consultation requirements should be explored as ways to mitigate these risks.

As explained in the responses to the consultation questions annexed to this response, the Home Office should also consider how the code of conduct and certification provisions within the data protection framework could support further codification of good practice and regulatory coherence.

Adequacy implications

There is potential for these changes to affect future EU assessments of the UK's data protection adequacy. The EU could determine that the UK no longer meets adequacy standards if:

- our oversight of the processing of personal information by law enforcement organisations were reduced; or
- the new framework were seen to weaken existing protections.

Government should keep this risk under close review, as losing adequacy would significantly undermine effective cooperation and data sharing with counterparts in the EU. These capabilities are essential for preventing and detecting crime and protecting public safety.

Annex One

ICO response to specific consultation questions

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?**

   Agree

As noted in the consultation document, there is ongoing concern and public debate about the state's powers to collect and process citizens' biometric data and on whether police are acting proportionately. Our research found that the public generally accepts police use of FRT, but this is conditional on appropriate safeguards, accuracy, and responsible use.

Greater clarity, certainty and specificity in the legal framework could help ensure public confidence in the use of these technologies and the safeguards that are in place. This, in turn, can help people to hold organisations to account, challenge and seek redress where things go wrong. It will also support effective and efficient regulation by relevant oversight bodies, including the ICO.

A new framework should consider the breadth of FRT, biometric and similar technologies law enforcement organisations use or are likely to deploy for law enforcement purposes. However, data protection law already applies to all processing of personal information, including processing which uses biometric technologies, through a principles-based and technology-neutral framework that can adapt as society and technology evolves. Therefore, even if a new framework is not comprehensive, existing data protection safeguards will continue to apply. These provide strong foundations for ensuring biometric technologies are used lawfully and proportionately.

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?**

   Yes, the legal framework should apply to technology which can make inferences about a person's emotion and actions.

We have expressed concerns about inferential technologies and the significant risk of unwarranted outcomes for the people concerned. In our view, a greater degree of legal specificity is necessary to address when and how these technologies can be used, and whether additional safeguards are appropriate beyond those in the data protection legislation.

We commissioned an Omnibus survey on biometric technology that found (at question 11) that a high proportion of people surveyed (40%) were uncomfortable with inferences or predictions being made about them based on their observed behaviour. An identical proportion raising concerns around this technology making predictions about their emotional state (40%).

Our Biometrics foresight report identified the deployment of emotional AI as an area of high risk. This may reveal highly sensitive information via subconscious behaviours and responses, interpreted through highly contested forms of analysis.

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)?**

   Yes, the legal framework should apply to technology that can identify objects linked to an individual.

If the purpose of using technology in this way is to identify or make decisions about particular people, this will amount to the processing of personal information regulated by data protection law. We consider that such use, particularly by law enforcement agencies, can have a significant impact on the people concerned. It would therefore benefit from a greater degree of specificity in when and how it can be used.

4. **Do you think that the types of technology the legal framework applies to should be flexible to allow for other technology types to be included in future? The alternative would be for Parliament to consider each new technology.**

A new framework will only increase clarity and confidence if it provides more specificity about particular technologies than the existing principles-based data protection framework.

If the framework is general enough to cover all existing and future biometric technologies, there is a risk it might not add any or much value beyond the existing data protection framework. It could also lead to contradictory outcomes through divergent interpretation of those frameworks.

It is likely to be challenging to ensure full coverage in a more detailed legislative framework from the outset, given the potential for new technologies to develop over time. It is therefore important for the government to develop a framework that builds in mechanisms to review, add and amend details over time. Codes of practice, such as those allowed for in data protection legislation, are likely to offer flexibility. But questions can arise about their status and enforceability by regulators, which can make oversight challenging and regulatory decisions open to substantial and lengthy legal challenges. Secondary legislation or rule-making powers may offer greater flexibility but with a lower risk of legal challenge. However, further work is required to explore the risks and benefits of these approaches as the proposed framework develops.

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?**

   Neither agree nor disagree

Government's priority should be to establish a clear and effective framework for law enforcement use of biometric and facial recognition technologies. It should recognise that such processing can significantly affect large numbers of people, including restricting people's liberty. To maintain public confidence, the legal framework and its oversight arrangements must be robust, transparent and clearly understood.

However, to ensure the framework is effective, the Home Office should consider the range of ways in which law enforcement agencies may use and deploy technologies. This includes where this is in partnership with others. These can include:

- procuring technology and using it to interrogate police information and databases;
- using third-party search services; and
- collaborating with other organisations to share technology or infrastructure and information for law enforcement purposes.

Further consideration is also needed where non-law enforcement bodies' legal obligations to protect the public and prevent and detect crime may

lead them to adopt such technologies that will require collaboration with the police or use of law enforcement information, or both.

Wider use of FRT in non-law enforcement contexts raises broader policy questions and would require further consultation and parliamentary scrutiny. Some proposals could introduce uncertainty, such as a wider 'have regard to' approach, under which organisations would not be legally subject to the framework but would take it into account when considering their own practices. This is unless they were supported by clear detail on how this would operate in practice, including on regulatory remits, supervision and enforcement action. All of which would need to be clearer before reaching a view on the merits of this option.

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?**

To ensure that the new framework is compatible with data protection legislation, we would expect its content (or alternatively the content of any codes of practice) to be fully and robustly tested against data protection requirements, including (but not limited to) consideration of the following:

- Whether the same result could be achieved by other, less intrusive means (data minimisation, proportionality).
- Whether the biometric or inferential technology is actually effective in achieving the intended aim (strict necessity).
- What people's reasonable expectations are around the use of technology (fairness).
- In the case of inferences, the action taken based on the inference.
- The length of time the data is stored for (storage limitation).
- Whether any automated decisions are made (ie without human oversight).
- The potential for reusing images or associated information.

We commissioned research by Revealing Reality on Understanding the UK public's views and experiences of biometric technologies that indicated concerns about accuracy. Participants' concerns were particularly focused

on situations where facial recognition technology might affect people's legal rights, liberty or reputation. The research found that the key factors that influence public comfort with police use of FRT include:

- the belief that society benefits from the technology;
- perceptions of accuracy; and
- holding positive views of the police.

People who agree with these ideas are substantially more comfortable with its use. Conversely, concerns about civil liberties, privacy, bias, and lack of transparency correlate strongly with discomfort.

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?**

In addition to the factors listed above, it is also relevant to consider the following:

- the nature of the space where the technology is deployed, the nature of the activity that is going on in that space (and who is doing it – ie children).
- Whether the technology is used pre-emptively, live or after the event.
- The nature or extent of the interference with other rights and the impact this is likely to have on the people whose information is used.
- The nature of the right interfered with (ie is it an absolute right or a qualified right).
- The extent of any safeguards around the use of the technology, (eg right to an appeal or review or human involvement in any decision).
- Transparency around the use of the technology and the consequences of its use.

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?

Agree

The seriousness of the harm that the use of the technologies is seeking to mitigate would be a relevant factor in assessing the fairness and proportionality of processing of personal information. We think it would also be a relevant factor here. This is because this framework would provide a further layer of specificity about the use of people's information than that provided by the general data protection framework.

From a public perception perspective (as noted in our research), public support for use of these technologies (FRT) is at its highest for the clearest use cases related to the most extreme or serious examples of crime and public safety. This support decreases as these use cases become more open-ended and unclear.

Compliance with data protection law is most easily achieved when the purpose is specific, clear and limited. This allows the circumstances and specific risks to be more accurately assessed and mitigated.

9. **What factors do you think are relevant to assessing 'seriousness' of harm? For example: the type of offence that has been committed; the number of offences that have been committed; the characteristics of the victim; whether there is an imminent threat to life, or there is an urgent safeguarding issue.**

We agree with the factors listed as examples in the questions and consider that the likelihood of harm is also relevant. Data protection law is built on the basis that organisations must assess risks to rights and freedoms and develop appropriate mitigations. Data protection impact assessments provide a structured way to think about and manage the potential risks of proposed processing activities and the impact on people. Our Overview of data protection harms and the ICO's taxonomy also contains useful information about how we consider the concept of harm in a data protection context.

When making an assessment, we do not think that aggregating numerous minor harms across a wide population should justify intrusive use of the technology that results in significant harm to a small proportion of the population.

The commissioned research by Revealing Reality on Understanding the UK public's views and experiences of biometric technologies indicated that people were more comfortable with FRT being used after an incident had taken place, and for crimes they saw as more 'extreme'.

Comfort was highest when FRT was understood to be used to locate people suspected of a terrorist act (83% comfortable). Levels of comfort were also high for finding a person reported as missing (83% comfortable); murder investigations (82%); and suspected theft or burglary cases (78%).

However, comfort levels were slightly lower for types of investigation that might be perceived as less 'extreme' or more 'open-ended'. 71% felt comfortable with its use to investigate public disorder. Just 65% felt comfortable with using FRT to find people who the police suspected were about to commit a crime.

The research did not provide definitions for types of policing activity, so some of these attitudes could have been based on perceptions of what is involved in these activities, and how they play out in practice.

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.

Agree

Generally, the higher the risks to people's rights and freedoms that arise from the use of the technologies, the greater the need we think there is for additional safeguards. Data protection law reflects this approach. It is based on balancing the benefits of processing personal information in pursuit of legitimate interests and aims against the risks to the rights and freedoms of those whose information is used. Organisations must think about and mitigate those risks prior to processing. Where they cannot be sufficiently reduced, they must consult the ICO prior to starting the processing. Where we have concerns about intended processing, we have regulatory powers that we can exercise, including issuing warnings. If processing commences, we can issue reprimands or enforcement notices that can require organisations to cease processing, amongst other things.

Given the different elements of law that these reforms are seeking to bring together, it may be appropriate to have different levels of authorisation. But this will depend on what specifically is being assessed and approved and where the appropriate level of knowledge, expertise and accountability can and should be brought to bear. As noted, there are already requirements to consult the ICO about high-risk processing and more generally to demonstrate accountability for any processing of personal information under data protection law. This should be based on input from data protection officers.

The efficacy of including different and specified levels of authorisation within the law enforcement ecosystem is a question we think best answered by those with in-depth knowledge of accountability schemes within law enforcement agencies. We would also suggest that the government will need to provide more detail on the specific uses and authorisation levels they have in mind in order to properly address this question. This includes articulating how the authorisation approach would differentiate between approvals for a specific operational use of approved systems or technology, and the commissioning or use of a new or novel technology.

We commissioned research by Revealing Reality on Understanding the UK public's views and experiences of biometric technologies. We found that nearly half (48%) of respondents felt that current regulation of police use of FRT is appropriate. Although a sizeable 38% remained neutral, suggesting limited awareness of existing regulatory frameworks. While 91% believed all UK police forces should follow the same rules about FRT use, only 42% thought this was currently happening.

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.

See answer to question 10.

12. If law enforcement organisations were not able to identify a person using law enforcement records and specific conditions were met, the systems could be enabled in such a way as to enable them to biometrically search other Government databases, such as the passport and immigration databases. In what circumstances should

biometrics searches of other Government databases be permitted?

Circumstances	Yes	No	Don't know
Searches should be for 'serious' offences.			
Searches should be for a safeguarding purpose (eg a suspected missing or vulnerable person).			
Searches should be to identify injured, unwell or deceased people.			

Whether and when access to other government databases is, or should be, permitted by law enforcement is a complex issue. If access is to be broadened, we believe that this requires further analysis and Parliamentary debate.

As noted elsewhere, our public research found that levels of comfort with FRT being used were highest after an incident had taken place, and for crimes perceived as more serious or 'extreme'. However, the rapid development of technology and varied approaches to deployment will pose different risks. We understand that the capability to search other databases would be a powerful tool for retrospective facial recognition (RFR) and Officer initiated Facial Recognition (OIFR).

The level of detail given here is not sufficient to allow a properly informed assessment of this question. We suggest that the 'specific conditions' in which it is envisaged that searches might be permitted would need to be

fully and robustly tested against data protection concepts. This would include the data protection principles such as fairness, compatibility and, where relevant strict, necessity.

13. If biometric searches of other Government databases take place, what safeguards should be in place?

Safeguards	Yes	No	Don't know
Search requests should be approved by a senior police officer or other appropriately qualified person			
Search requests should be approved by an independent body.			
Search records should be kept for review by a senior police officer or other appropriately qualified person			
Records should be kept for review by an			

independent body.			

Are there any other limitations or safeguards you think should be considered?

The appropriateness of additional safeguards to guard against excessive or unnecessary data collection, whether proactive or reactive, will depend on the context and nature of the data and the potential impact that processing would have on people. Parliamentary scrutiny of any legislative safeguards will be necessary to ensure that they are fair, transparent and effective.

The nature of FRT and the way it is deployed is also likely to affect what safeguards are appropriate. For example, in the case of Officer Initiated Facial Recognition (OIFR), there is significant discretion and responsibility afforded to individual officers. Often they are working with limited information to base their decision on and they could potentially seek access to a range of databases. It may be appropriate to seek authorisation from a more senior or appropriately qualified person in these circumstances. From a data protection perspective, it is also relevant to consider input from the data protection officer.

Under the DPA, law enforcement organisations must also maintain logs which act as a digital footprint and record the actions of users in automated processing systems. This is an internal accountability mechanism and provides a record of how somebody has used personal information within a system. As a minimum, logs must be kept for collection, alteration, consultation, disclosure, combination and erasure. Further consideration should be given to the protection that logging requirements offer when determining what additional safeguards are appropriate.

14. The functions set out above could be undertaken by one single independent oversight body – do you agree? This could be achieved by them overseeing multiple codes of practice (see also questions 15 and 16).

Disagree

As noted elsewhere, data protection law applies to all processing of personal information. Therefore any technology which processes personal information is subject to data protection rules. If law enforcement agencies use FRT or biometric technologies to identify living people, this use is governed by data protection law and falls within the regulatory remit of the ICO.

Data protection law must remain central to the governance of biometric technologies. It provides crucial protections, requiring organisations to balance law enforcement objectives with people's rights and freedoms. These laws are technology-neutral and designed to interact with other statutory frameworks. Any new regime must build on these foundations rather than replace them.

See annex two for further information about the ICO's regulatory functions, tasks and powers, including our complaints handling and personal data breach reporting tasks and our role in ensuring appropriate data security.

In principle, we have no objection to the proposal to merge the roles of the BSCC and the FSR. However, it will be important to consider how this interacts with the ICO's role should the new body be given:

- additional powers;
- the ability to set out regulatory requirements in codes of practice; and
- duties to ensure that law enforcement organisations are using FRT and biometric technologies responsibly.

In particular, we are keen to ensure there are no contradictions between the expectations of law enforcement bodies under data protection law and any requirements set out by the new body, and that it is clear how and when each body would exercise its powers.

Statutory consultation duties and memoranda of understanding (MoUs) will likely be required to ensure coherence and complementary ways of working across regulatory remits.

15. What sort of powers or obligations should the oversight body have to oversee law enforcement use of facial recognition and similar technologies?

New legal framework for law enforcement use of biometrics, facial recognition and similar technologies

	Yes	No	Don't know
Publish codes of practice detailing what law enforcement organisations would be expected to do to meet their legal and ethical obligations when developing or using technology			
Investigate instances where use of a technology presents substantial risks to criminal investigations or proceedings due to non-compliance with the code of practice.			
Investigate instances where use of a technology has potentially unjustified interferences with the rights and protections people have under data protection, equalities and human rights law			
Investigate instances where a technology has been misused, hacked or accessed without authorisation.			
Request information from law enforcement organisations to aid oversight of police use of the technology			
. Issue compliance notices requiring law enforcement organisations to take specific actions to remedy noncompliance			
. Seek injunctions to prevent or stop technology use that pose significant risks, in conjunction with other statutory bodies where necessary.			
Make public declarations about non-compliance to inform stakeholders and the public.			
Receive complaints and referrals from anyone, in order to inform their investigations.			
Publish an annual report detailing compliance with the relevant Code(s) of			

practice and recommendations to Parliament on revisions to the Code.			
Set standards that help assure the scientific validity of the technology Decide which new technologies or new uses of existing technologies should be added to the legal framework in future.			

What other powers or obligations do you think there should be?

Please see our response to question 14 and the further detail about our functions, tasks and powers in annex two. The new framework should avoid duplicating existing tasks and functions. We should retain responsibility for data protection requirements and MoUs should be explored to establish ways of working in areas where remits intersect in complex ways.

Data protection is not well placed to address technical standards in isolation and would benefit from collaboration.

To the extent that any revised framework relies on codes of practice, it will be important to clarify their status and the responsibility for oversight. Codes of practice are generally not directly enforceable, and action is usually grounded in breaches of the underlying legislation that they are based on. Further exploration of roles and responsibilities of respective regulators will be needed as the proposed reform approach develops.

The data protection legislation provides for codes of conduct and, for processing under UK GDPR, certification. Government should explore how this could contribute to the proposed reforms and assist with defining consistent sector-specific practices that are approved by us.

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?

Neither agree nor disagree

It is likely that bias and discrimination will be an area of ongoing shared regulatory interest between any new oversight body, the ICO and the Equality and Human Rights Commission (EHRC). Codes of practice developed by the Secretary of State, in collaboration with all parties, could support a coherent regulatory approach. These have the potential to clarify specific practices required to address and mitigate bias and discrimination which we would then take into account when fulfilling our functions and tasks.

17. What types of rules might the new oversight body be responsible for setting? These could include ensuring tools are of sufficient quality or determining what testing should be undertaken.

Our guidance on biometric data and AI and data protection address how data protection law applies to the use of biometric recognition systems and other AI tools. This includes how the statistical accuracy of systems relates to the fairness principle and how to mitigate the risk of discrimination. Whilst not specifically aimed at law enforcement organisations, many of the concepts are still relevant.

The new framework should build on existing regulatory obligations, including data protection requirements and guidance, to create greater specificity and clarity in a law enforcement context. For instance, this could include requirements around testing of technical performance and statistical validity, as well as for procuring and deploying new and emerging technologies.

Collaboration with standards communities, deployers and testers, as well as other relevant regulators, will be beneficial when setting these kinds of rules. Collaboration through regulatory sandboxes could play a role in providing assurance, as could participation in global technology standards and evaluations (such as NIST's FRTE project).

Government should also assess the role that certification (including data protection specific schemes) could play, in conjunction with procurement frameworks. This could support efficient and effective due diligence and selection of biometric technologies by law enforcement bodies.

Annex two: ICO powers and functions

Advisory functions

- Providing input to government and Parliament about the implications of legislative and regulatory proposals affecting the processing of personal information.
- Providing expert advice to government on making adequacy regulations for third countries receiving international transfers from the UK.
- Supporting organisations by providing advice and guidance about how to comply with data protection law. This includes where organisations are obliged to consult the ICO about certain processing where they cannot mitigate the risks.

Complaint handling and redress

- Handling complaints raised by people where they have an issue about their personal information or are unable to exercise their information rights.
- Receiving reports of, and investigating, personal data breaches.

Approval functions

- Considering and approving codes of conduct brought forward by organisations. Codes of conduct are voluntary accountability tools, enabling sectors to identify and resolve key data protection challenges in their sector with assurance from the ICO that the code, and its monitoring, is appropriate. They have been extended to law enforcement organisations under the Data Use and Access Act.
- The Secretary of State can instruct the ICO, using secondary regulation making powers, to develop and issue codes of practice. These set out our expectations for complying with data protection law in a specified area. We must take these into account when considering whether relevant organisations have complied with their data protection obligations.
- Approving administrative arrangements and managing and monitoring international transfer notifications received from competent authorities.

Investigative and corrective functions

- Information notices (requesting specific information or documents).
- Assessment notices (compulsory audits) as well as a programme of voluntary audits, which provide recommendations on improving data protection practices.
- Enforcement notices (formal directives requiring organisations to address breaches of data protection law).

- Reprimands (formal notice to an organisation that has infringed data protection law. This can include recommended or required action that they must undertake to address the infringement).
- Penalty notices (monetary fines).
- Prosecuting criminal cases where proof of unlawful access, disclosure or deletion is found.
- Under the Data (Use and Access) Act, we will soon have additional powers, such as compelling a witness to attend an interview and the ability to commission a technical report.