



Home Office

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

Government consultation

This consultation begins on 04 December 2025

This consultation ends on 12 February 2026

About this consultation

- To:** Representations are welcome from professional bodies, interested groups and the wider public
- Duration:** From 04/12/2025 to 12/02/2026
- Enquiries and responses to:** New legal framework consultation
Data & Identity Directorate
2 Marsham Street, 1st Floor, Peel Building, London, SW1P 4DF
Email: fr-consultation@homeoffice.gov.uk
- Additional ways to respond:** A series of stakeholder meetings is also taking place. For further information please use the 'Enquiries' contact details above.
- Response paper:** A response to this consultation exercise is due to be published within 12 weeks at <https://www.gov.uk/government/consultations/legal-framework-for-using-facial-recognition-in-law-enforcement> .

Contents

Consultation on a new legal framework for law enforcement use of biometrics, facial recognition and similar technologies.	2
Ministerial foreword	2
Executive summary	4
Consultation on a new legal framework	7
About you	24
Contact details and how to respond	25
Complaints or comments	25
Extra copies	25
Publication of response	25
Representative groups	25
Confidentiality	25
Consultation principles	27

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

Ministerial foreword

Facial recognition technology has shown itself to be a valuable tool to modern policing. Between September 2024 and September 2025, the Metropolitan Police recorded 962 arrests for offences including rape, domestic abuse, knife crime, grievous bodily harm (GBH), and robbery as a direct result of using live facial recognition to locate people. Over a quarter of these arrests related to offences involving violence against women and girls. In response to the summer disorder last year, the use of retrospective facial recognition led to 127 arrests. This, and other similar technologies, have significant potential to help deliver the Government's Safer Streets Mission.

But I understand there are legitimate concerns about this powerful technology. There are questions we must address about the state's powers to process its citizens' biometric data, and about public confidence in the police to act proportionately. And we know some people have significant doubts about this. That is why, over the past year, we have taken time to listen carefully to all sides of the debate about facial recognition and evaluate the available evidence.

We know from discussions with police officers how this can be a valuable tool in tackling serious crime, and we have heard many examples of successes from its use. We have also listened to civil society groups, academics, and regulators who raised important questions about oversight, transparency, and the risk of bias.

On public trust, the indications are that there is support for the police to use the technology, if it is used with the necessary safeguards. The Home Office has conducted a national survey to explore public attitudes in detail, and I am encouraged by the findings, which are published alongside this consultation.

After careful consideration, whilst it is clear there is a legal framework within which facial recognition can be used now, I believe that confident, safe, and consistent use of facial recognition and similar technologies at significantly greater scale requires a more specific legal framework. This will ensure law enforcement can properly harness the power of this technology whilst maintaining public confidence over the long term.

In the more specific legal framework, we must ensure we balance the seriousness of harm the police are seeking to detect or prevent with individual rights, as well as how the use of technology is independently monitored. We must also ensure the framework is resilient to future technological developments.

Your responses to this consultation will be invaluable in helping us to establish an informed, robust, and future-focused specific legislative regime.

Thank you for your engagement and your commitment to this important work.

Sarah Jones MP
Minister for Policing and Crime Prevention

Executive summary

The UK Government is launching a consultation to help develop a new legal framework for the use of facial recognition and similar technologies by law enforcement. While these technologies have already proven valuable in tackling serious crime and enhancing public safety, their use raises important questions about privacy, oversight, and public trust. The established legal basis for use of these technologies is derived from a patchwork of common law, data protection, and human rights legislation. This consultation aims to ensure that the law keeps pace with technological developments and provides clear, consistent rules that the public can understand more easily, and that police can rely on as they increasingly use these technologies.

The consultation seeks views on a wide range of issues, including which technologies should be covered by the new framework - such as biometric, inferential, and object recognition tools - and which organisations it should apply to. It also explores when and how these technologies should be used, what safeguards are necessary to protect privacy and other rights, and how to ensure their use is demonstrably proportionate to the seriousness of the harm being addressed. Key questions include whether certain uses should require higher levels of authorisation or independent oversight, and under what conditions law enforcement should be allowed to search other Government databases using biometric tools.

Another major focus is on accountability and fairness. The Government proposes creating a new oversight body to consolidate and clarify existing regulatory roles, ensuring responsible use of these technologies. This body would be empowered to set standards, investigate misuse, and enforce compliance. The consultation also addresses the need to guard against bias and discrimination, proposing that law enforcement agencies follow specific rules and testing protocols to ensure equitable use. Public input will be vital in shaping a legal framework that balances innovation in policing with the protection of individual rights and freedoms.

A new legal framework fit for the 21st Century

DNA was first used in a criminal investigation in 1986, and the first UK conviction using fingerprint evidence was in 1902. The police still use these biometric technologies every day; to identify offenders, solve cold cases and exonerate the innocent. The use of photographs by the police has an even longer history; by 1872 over 43,000 photographs were collected across England and Wales, forming the basis of early criminal records. CCTV use goes back to the Metropolitan Police's deployment of temporary cameras in Trafalgar Square in the 1960s. Since then, video surveillance has become an integral part of urban infrastructure and an invaluable tool in the prevention and detection of crime. A national retrospective facial recognition tool has been available since 2014, to help identify individuals who are wanted, missing or vulnerable. Live facial recognition cameras are used in England and Wales to help find wanted people in public spaces. Camera quality is better than ever before, and face matching algorithms are faster and more accurate.

The Government's Safer Streets Mission is committed to halving violence against women and girls and knife crime in a decade and restoring confidence in our police service. For the Mission to succeed we must ensure the police have the systems and technology they need to tackle crime and the adoption of new technologies must be done in a way that is consistent, safe and fair. For powerful and complex technologies like facial recognition, it is important that rules about when, where and how law enforcement organisations use them are clear enough for the public to understand and the police to follow. Alongside a new legal

framework, policing structures need to support consistent, safe and fair use of technology. The organisational reforms needed to achieve this are not the subject of this consultation but will be part of broader police reform.

Parliament has already set out rules for the overt (visible) taking, retention and use of DNA and fingerprints, as well as when law enforcement organisations can take photographs. But these rules have not stood the test of time. They were written before computers could quickly and accurately carry out ‘facial recognition’ and ‘matching’. Although there is a legal basis for the police to use facial recognition technology for law enforcement, this relies on common law powers and a patchwork of equalities, human rights and data protection laws, as well as police guidance. For example, a member of the public living in Croydon would typically have to read four pieces of legislation and a police national guidance document, which is supplemented by detailed local force policy, legal documentation and impact assessments to fully understand the basis for the use of live facial recognition on their high street.

You can find more information about the current laws governing police use of facial recognition in our [factsheet and guidance](#).

We have been collecting evidence about law enforcement organisations’ use of facial recognition and similar technologies to better understand the benefits for keeping our streets safe as well as concerns about privacy, discrimination and the lack of a specific legal framework. We have commissioned a formal evaluation and have been listening to stakeholders. We have also held a series of roundtable meetings with law enforcement organisations, regulators, research institutions, civil society groups and industry.

We have been gathering the public’s views about the use of technologies like facial recognition. The findings from the first part of our evaluation work, published alongside this consultation, show that two in three people support police use of facial recognition technology. However, many also expressed concerns about the misuse of the technology and the risk of false identification.

We also welcome recent reports, such as the ‘Independent legal review of the governance of biometric data in England and Wales’ (2022) led by Matthew Ryder KC; the Ada Lovelace Institute’s report ‘An Eye on the Future: A legal framework for the governance of biometric technologies in the UK’ (2025); and the Alan Turing Institute’s Centre for Emerging Technology and Security report ‘The Future of Biometric Technology for Policing and Law Enforcement: Informing UK Regulation’ (2024).

We have concluded that although there is a legal framework for police use of facial recognition, it does not give the police sufficient confidence to use it at significantly greater scale. Nor does it consistently give the public the confidence that it will be used responsibly according to clear rules. This is because the current framework is complicated and difficult to understand. **The Government is therefore committed to developing and introducing a new legal framework that sets out rules for the overt use of facial recognition by law enforcement organisations.**

Although police use of facial recognition has prompted the Government to examine the law in this area, other technologies with similar characteristics pose similar questions, such as in what circumstances can their use be justified? This consultation therefore asks more broadly about principles that could be applied to a wider range of technologies, which all have the potential to interfere with people’s rights. We will consider whether the new legal framework should extend to the use of other biometric and inferential technologies.

We will use the views gathered through this consultation, alongside other evidence, to draft a legal framework. This framework will set appropriate limits and safeguards on the use of facial recognition, ensuring that law enforcement organisations in England and Wales - and throughout the United Kingdom on reserved matters such as national security - strike the right balance between protecting our communities from crime and disorder, and safeguarding individual rights.

Any covert (secret) uses of these types of technology would be subject to a strict legislative regime, notably in the Regulation of Investigatory Powers Act 2000, and are not part of this consultation.

Consultation on a new legal framework

Objectives

Our objectives are that the new legal framework will:

- **Be accessible and transparent** – ensuring law enforcement organisations and the public can easily understand it and foresee how data and the technology will be used.
- **Set clear limits on law enforcement authority** – defining limits on decisionmakers' discretion (e.g. on questions such as when facial recognition can be used or who can be on a watchlist) and guarding against misuse.
- **Clearly define who sets rules, standards, and checks compliance** – consolidating and simplifying oversight and regulation.
- **Support technological development** - by being consistent on when the use of biometric and similar technologies that may interfere with individual rights can be justified, making the framework more 'future proof' than existing legislation.

Which technologies should the new framework apply to?

There are three main uses of facial recognition technology currently available to the police.

Live facial recognition involves processing live video footage of people passing a camera. The images are compared against a specific watchlist of wanted people. In the event of there being no match, the image is deleted immediately. Where there is a potential match, a police officer decides whether to engage with the individual. Ten police forces in England and Wales have used this technology.

Retrospective facial recognition is used after the event and is a common feature of police investigations. Images of people the police need to identify are taken from crime scenes, typically CCTV or mobile phones, and compared against custody images of people who have previously been arrested. Over 25,000 searches using retrospective facial recognition are carried out each month on the Police National Database and some police forces have their own local systems.

Operator-initiated facial recognition is a relatively new capability and is only being used by two police forces. It is a mobile app which allows officers on the street to conduct an identity check against the custody image database, without having to take the person being checked into custody.

These use cases are all covered by this consultation, although the consultation questions do not make a distinction between the different uses, focusing instead on the ways, the purposes and the circumstances in which the technologies can or should be used. This is because the new legal framework will need to be applicable to all existing and possible uses of facial recognition, acknowledging that the interference with individual rights is likely to vary depending on a range of factors.

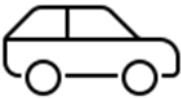
This consultation has been driven by a desire for specificity and consistency in the laws governing the use of facial recognition technology by law enforcement organisations. There are, however, other similar existing and developing technologies that may benefit from the same type of framework.

Many of these technologies are driven by 'biometric' data or processing that can enable a machine to make an inference about a person based on their physical actions. 'Biometric data' is defined in the Data Protection Act 2018 as "personal data resulting from specific

technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allows or confirms the unique identification of that individual". For example, technology that can help law enforcement organisations to identify unknown individuals using unique characteristics like their voice or the way they walk.

The new framework could also cover technologies designed to identify specific motions or emotions, for example, technology to help police spot behaviour associated with criminal activity or for public protection, such as suicidal intent. Additionally, it could cover technologies that do not use biometric data but can identify personal objects like bags, shoes and jackets, and bigger items like cars.

*Table 1: Facial recognition and examples of other technologies which **could** be subject to a new legal framework when used by law enforcement organisations.*

Biometric technologies match:	Inferential technologies look for:	Object recognition matches:
Fingerprints  DNA  Faces 	Being untruthful in a polygraph  Collapsed or injured  Pacing a suicide hotspot 	Hats  Vehicles  Bags 
Other examples of emerging biometric technologies include voice and iris recognition. For examples of uses of facial images, see our facial recognition factsheet and guidance.	Example: technology analysing people's movements runs on live CCTV at a known suicide hotspot. It sends an alert to a police station when an individual repeatedly paces the area.	Example: police use technology to retrospectively search hundreds of hours of CCTV footage from a high street to identify the route of an individual wanted for a violent offence wearing a specific colour and style of jacket.

When formulating the new legal framework, the Government will need to set clear parameters for the types of technology which will be subject to the legislation, including safeguards and limits.

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	Neither agree nor disagree	Disagree	Don't know

Please explain your answer

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.	No, the legal framework should not apply to technology which can make inferences about a person's emotion and actions.	Don't know

Please explain your answer

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.	No, the legal framework should not apply to technology that can identify objects linked to an individual.	Don't know

Please explain your answer:

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.

Yes, the types of technology the legal framework applies to should be flexible	No, the types of technology the legal framework applies to should not be flexible	Don't know

Please explain your answer:

Which organisations should the new framework apply to?

We propose that the new legal framework will only apply to law enforcement organisations. This includes all police forces in England and Wales, and national and specialist law enforcement agencies like the British Transport Police and National Crime Agency and for law enforcement activity by other public bodies such as the Environment Agency, HMRC or Border Force.

However, we recognise that facial recognition and similar technologies are used more broadly across the public and private sectors and that sometimes this is to prevent crime or to protect people. For example, shops use facial recognition technology to help identify known or suspected shop thieves, and nightclubs use it to help identify barred patrons. If public and private sector users are excluded from the scope of the new legal framework they would still have to comply with all relevant existing legislation including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 and guidance, with the Information Commissioner's Office (ICO) as the principal regulator. We will consider whether public and private sector organisations ought to have due regard to the new legal framework and especially to any best practice established as a result.

The Government proposes that the new legal framework should focus on the use of facial recognition and similar technologies by law enforcement organisations, for a law enforcement purpose. A law enforcement purpose is defined by section 31 of the Data Protection Act 2018 as:

- prevention of criminal offences;
- investigation of criminal offences;
- detection of criminal offences;
- prosecution of criminal offences;
- execution of criminal penalties; and,
- safeguarding against, and prevention of, threats to public security.

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?

Agree	Neither agree nor disagree	Disagree	Don't know

Please explain your answer:

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

How should the framework protect people's privacy?

Use of biometric data of individuals will always involve some degree of interference with people's rights, such as the right to privacy. For subjects of a police investigation, the Police and Criminal Evidence Act 1984 clearly explains when this interference is justified for DNA and fingerprints, setting out the circumstances in which law enforcement organisations can take, retain, and use someone's DNA or fingerprints. In most circumstances, when someone has been convicted of a criminal offence, it is considered appropriate (and lawful) to retain their DNA and fingerprints on a national database to identify them in future or to search them against unidentified DNA and fingerprints from crime scenes.

There could also be interference with the privacy of others who are not the subject of a police investigation. Interference would depend on the type of facial recognition or similar technology being used, but could include other individuals with facial images on the database being searched, or individuals walking past a camera that is undertaking live facial recognition.

There are also already rules for when other parts of Government can take, retain, and use biometrics-for example, for immigration purposes. The UK Borders Act 2007 defines how long biometrics may be retained when applications are made for most forms of immigration permission. All passport data, including facial images, is retained on the Passport Data Store for a period of 80 years, as an exercise of the Royal Prerogative.

Whilst there are rules governing when law enforcement organisations can take, retain, and use facial images (e.g. using facial recognition), they leave more space for discretion in the way they are applied and are not subject to specific statutory oversight, unlike DNA and fingerprints. The new legal framework must therefore clearly set out the circumstances in which law enforcement organisations can take, retain, and use facial images, including the use of facial recognition. This consultation asks questions about when the use of biometric and associated technologies could or should be considered both 'necessary' and 'proportionate' by law enforcement organisations.

We believe that the use of biometric and inferential technology should always be demonstrably 'necessary' and 'proportionate' to the objective being sought. A clear and consistent justification for interference with people's rights is required, and the burden of

threshold setting and decision making needs to be attributed to, and shared appropriately between, Parliament, Ministers, independent oversight bodies, and law enforcement organisations.

The Government believes that we need to take into account the following factors when assessing whether the interference with privacy caused by biometric and inferential technologies, such as facial recognition, can be justified. The nature of interference with someone's privacy will depend on:

- the seriousness of the harm the interference is seeking to prevent or detect;
- whether biometric data is acquired, retained, and searched voluntarily or involuntarily;
- whether biometric data is acquired, retained, and searched overtly or covertly; with or without explicit consent;
- whether biometric data is acquired and/or used in a public or a private space, and the nature of the public or private space;
- whether or not someone is the intended subject of a police investigation
- who has access to the data and the results;
- whether the biometric processing is used to locate, identify, or make inferences about people;
- whether biometric searching is likely to impact on a small or large number of people (e.g. the size and nature of the database or watchlist), and to what degree; and
- whether biometric data was acquired for another purpose, such as in connection with a passport application rather than law enforcement.

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?

Answer:

How should the framework protect other rights?

Facial recognition and similar technologies have the potential to interfere with other rights, such as the right to freedom of expression and the right to freedom of peaceful assembly. This could include the rights of those who are not the subject of a police investigation. Rights could be engaged if facial recognition were to be used at a protest or other public gathering, or on video footage obtained at such a gathering. In these cases, we want to ensure that any interference can be justified and is proportionate to the objective being sought. For example, we might deem there to be a sufficient level of seriousness to justify use of facial recognition in a situation where video footage taken at a protest captured a violent assault, or significant criminal damage occurring within the crowd. We could also consider whether the use of these technologies in advance of a protest or gathering could be justified if it helps to keep the event safe for the majority. Our objective is to make sure that the new legal

framework ensures the technology can be used in a balanced way, so that it does not deter individuals from expressing themselves freely or discourage participation in peaceful demonstrations or rallies.

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?

Answer:

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

The law already sets limits in terms of ‘seriousness’ in many policing scenarios. For example, when someone is convicted of a crime, there are sentencing criteria which vary based on the nature and seriousness of the offence. The seriousness of a public protection issue in England and Wales is determined by a combination of risk, vulnerability, harm, and threat. These factors are outlined in the College of Policing’s Authorised Professional Practice (APP) on Major Investigation and Public Protection.

Example 1

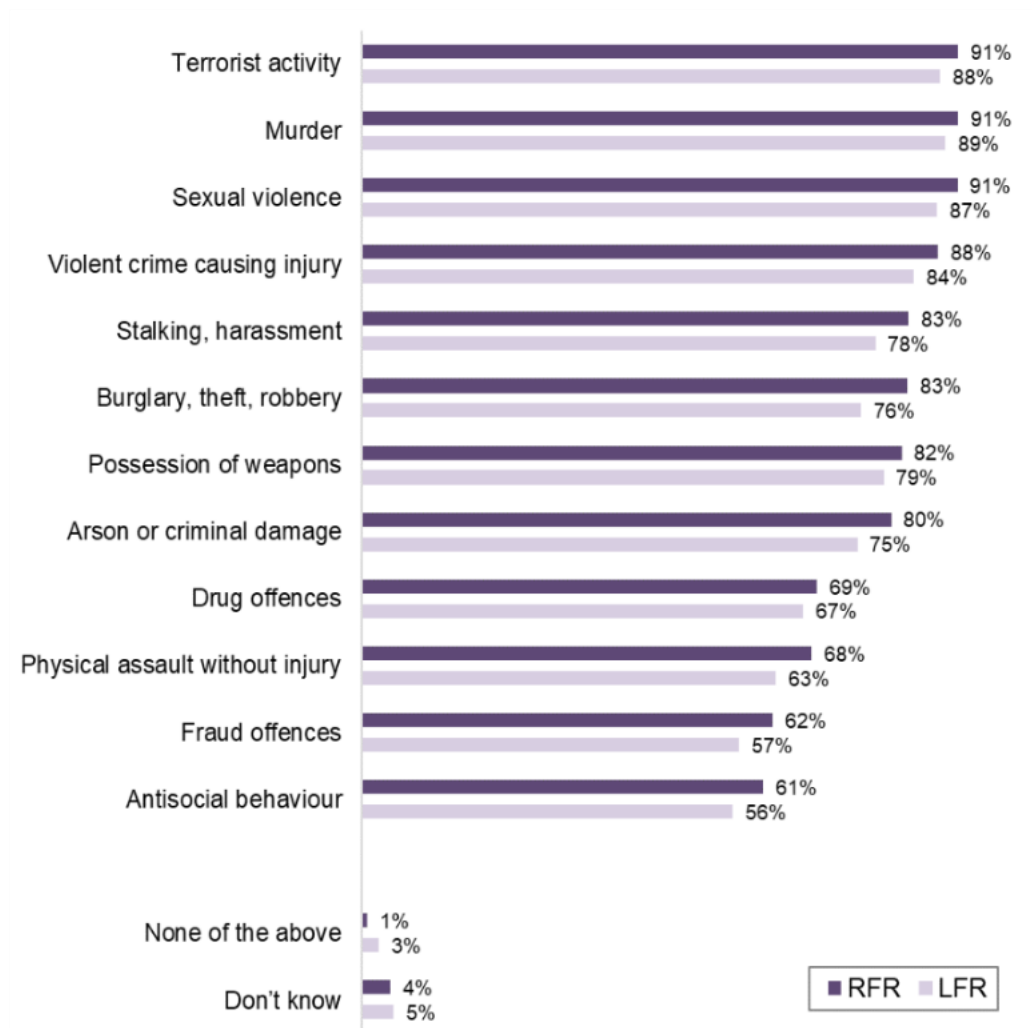
Qualifying Offences for Biometric Retention and Use

The length of time DNA and fingerprints can be kept and searched depends on whether a person was arrested for a qualifying offence. Qualifying offences include sexual, violent, terrorism and burglary offences. The Protections of Freedoms Act 2012 contains the rules for how long certain law enforcement organisations can retain and use DNA and fingerprints.

We know that public perception and acceptance of the use of facial recognition depends on the circumstances in which it is being used. Acceptance varies according to the seriousness of harm law enforcement organisations are seeking to prevent and detect, and the way in which the technology is being used e.g. whether it is being done in live time to search for a wanted person, to identify a person on the spot, or to identify someone alleged to have committed a crime after the event.

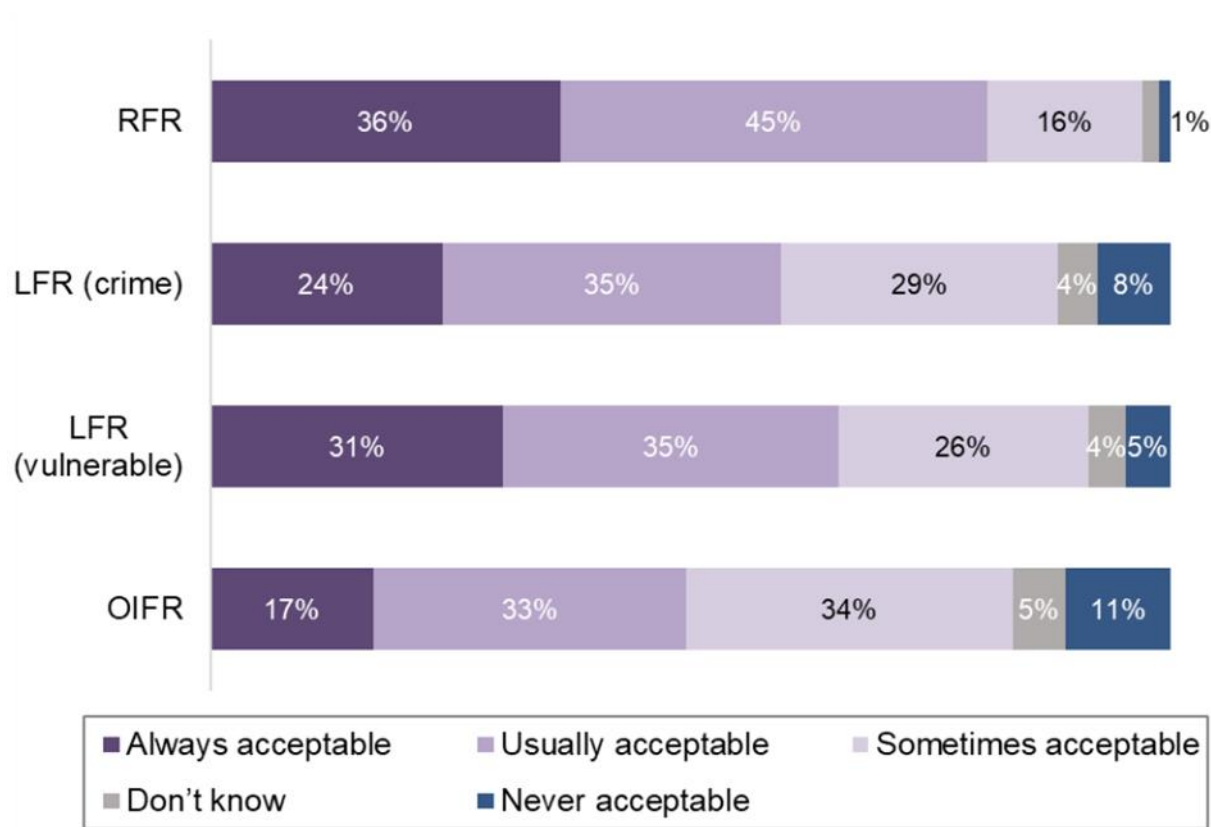
The Home Office has carried out a survey on public attitudes to police use of facial recognition*. Some of the results are set out in the table below.

Question: For which offences do you think police use of retrospective facial recognition /live facial recognition would be acceptable? Select all the options you think apply. Respondents: N=3,920; unweighted base.



*Home Office Public Attitudes survey.

Question: How acceptable or unacceptable do you think it is for the police to use facial recognition technology in the following ways: Retrospective facial recognition, live facial recognition for crime, live facial recognition for vulnerable people, Operator-initiated facial recognition technology? Respondents: N=3,920; unweighted base.



The new legal 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. For example, where there is an imminent threat to life, it might almost always be justified to use some or all types of facial recognition technology to prevent that harm. In other cases, the harm being prevented or detected may be considered less 'serious' and require a higher level of justification and authorisation.

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	Neither agree nor disagree	Disagree	Don't know

Please explain your answer

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.

Answer:

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

In some circumstances it will be appropriate for suitably qualified police officers, police staff, or other staff from law enforcement organisations to use technologies, such as facial recognition, without additional authorisation. In other circumstances, authorisation by a more senior police officer or suitably qualified person from an independent body may be required. The new legal framework will make this clear. The level of authorisation will vary, depending on the seriousness of harm law enforcement organisations are seeking to prevent and detect, as well as the potential interference with individuals’ rights, taking into account factors such as location, the origin of any data being searched, the number of people whose faces might be searched, and the urgency of the situation.

Example 2

Levels of sign off for use of live facial recognition

The College of Policing has published guidance for law enforcement organisations to follow when using live facial recognition technology [\[insert link here\]](#). The guidance says that authorisation to deploy live facial recognition in support of a policing operation should be made by an officer not below the rank of superintendent and should be recorded in writing.

In cases of urgency, force policy documents may provide that an officer below the rank of superintendent, but not below the rank of inspector, may authorise the deployment of live facial recognition in support of a police operation (e.g. where there is imminent threat to life or of serious harm to people or property, with limited time to act). An officer of the rank of superintendent or above must still be informed as soon as practicable and must authorise the deployment to continue or direct that it should stop.

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	Neither agree nor disagree	Disagree	Don't know

Please explain your answer

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.*

Answer:

Should law enforcement organisations be allowed to search other public records with this technology?

The Government collects, retains, and uses biometric data for other purposes. For example, His Majesty's Passport Office (HMPO) and immigration services collect facial images so that they can issue permissions to the right people and conduct fraud checks.

In some circumstances, law enforcement organisations can already request that the Home Office conduct searches of immigration and passport facial images if it has not been possible to identify someone from police records. This could be because of the seriousness of an offence, seriousness of a public safety issue, or for national security purposes.

A recent public attitudes survey conducted by the Information Commissioner's Office (ICO) found that levels of comfort varied slightly for different potential sources of images used for facial recognition.¹ The survey showed that 72% of respondents were at least somewhat comfortable for police to search UK immigration records, with 68% and 67% at least somewhat comfortable with law enforcement organisations searching the passport and driving licence databases respectively.

We want to make sure this type of searching, which has the potential to interfere more with people's privacy, is given particular consideration. **The Government is therefore consulting on the requirements and safeguards which should be in place before law enforcement organisations conduct biometric searches of other records held by the Government.**

Example 3

Biometric Searching of Other Public Records

Current technology enables law enforcement organisations to search immigration fingerprint databases as well as the fingerprints of people who have been arrested to help identify unknown individuals.² The same is not the case for facial images.

Home Office staff can search immigration and passport facial images on behalf of UK law enforcement organisations if certain criteria are met. Published policy states that Home Office staff must be satisfied that:

- the search is in the public interest
- the search is likely to achieve its aims
- all other reasonable alternative avenues with lesser intrusion have been exhausted before requesting a facial image search
- the intrusion on privacy rights is proportionate to the aim being pursued. To assist with this balancing exercise, the purposes for which searches can be conducted have been limited to areas where there are high levels of public interest (specifically serious crime, national security, and the protection of life); and
- the Home Office is lawfully able to share the results of any search.

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 (e.g. a suspected missing or vulnerable person).			
Searches should be to identify injured, unwell or deceased people.			

Answer:

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?

Answer:

Who should make sure law enforcement organisations are using this technology responsibly?

Oversight of police use of facial recognition technology is currently provided by regulators and public bodies, including the Biometrics and Surveillance Camera Commissioner, the Information Commissioner, HMICFRS, Equality and Human Rights Commission, and the Independent Office for Police Conduct. You can read more about oversight in [‘Police Use of Facial Recognition: A Guide’](#). We recognise that the oversight and regulatory landscape is complicated.

We believe that a structural change would make oversight more effective and propose creating a ‘one stop shop’ serving a common group of stakeholders with similar concerns and need for clarity.

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. More examples of the types of powers and obligations the new body could have can be found in question 15. The role of the new oversight body would be set out in law.

The Government proposes to create a regulatory and oversight body to oversee law enforcement use of biometrics, facial recognition and similar technologies. This is likely to encompass and build upon the existing roles of the Biometrics and

Surveillance Camera Commissioner and the Forensic Science Regulator in England and Wales.

Whilst validating the accuracy and performance of technologies is a common requirement, note that we are not proposing to change the way forensic science is regulated, as per the Forensic Science Regulator Act 2021, nor necessarily regulating all biometric uses in the same way as those used forensically.

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).*

Agree	Neither agree nor disagree	Disagree	Don't know

Please explain your answer

The powers and obligations of the new oversight body would be set out in statute. This consultation seeks the public's views on the powers and obligations the new body should have.

Example 4

Examples of the types of powers oversight bodies have

The Forensic Science Regulator ensures that the provision of forensic science services across the criminal justice system is subject to an appropriate regime of scientific quality standards. They have the power to investigate police forces and issue compliance notices where they deem the force is carrying on forensic science activities in a way that poses a substantial risk to the criminal justice system.

The Independent Office for Police Conduct oversees the police complaints system in England and Wales and sets and monitors the standards by which the police should handle complaints. They are responsible for investigating the most serious matters, including allegations of serious corruption, and cases where someone has died or been seriously injured following contact with the police.

The Information Commissioner's Office (ICO) is the UK regulator for personal data and has regulatory responsibility for biometrics captured, retained and used by HM Passport Office and UK Visas and Immigration. The ICO has the power to issue enforcement notices and penalty notices (administrative fines) where a data protection breach has occurred.

15. What sort of powers or obligations should the oversight body have to oversee law enforcement use of 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 non-compliance.			
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?

Answer:

How should the new framework guard against bias and discrimination?

However accurate biometric technologies can be, their performance is subject to many variables-such as the quality of the biometric sample, the number of years between the comparison biometric sample and the database sample, and the number of biometrics in the database. In the case of facial matching, in some matching algorithms, the age, gender and race of the individual can impact the results. This can affect the fairness-or 'equitability'-of any search results.

When biometrics such as DNA and fingerprints are used evidentially, their quality is subject to statutory regulation (Forensic Science Regulator Act 2021). The results are subject to detailed analysis and interpretation.

The Government already requires that all facial recognition algorithms used by law enforcement organisations that are funded by the Home Office are independently tested for equitability and bias. All police forces are also required to fulfil their Public Sector Equality Duty requirement to understand any bias in the technologies they are using.

Example 5

Equitability Testing by the National Physical Laboratory

The National Physical Laboratory (NPL) is a world-leading centre of excellence that provides cutting-edge measurement in science, engineering and technology. Over the last year, the NPL has conducted independent testing of the facial recognition technology used by specially trained operators in all police forces for retrospective facial recognition.

The testing gives an impartial, scientifically underpinned, and evidence-based analysis of the performance of the current facial recognition algorithms, and its future replacement. The reports have been used to update training for operators to better understand the performance of the retrospective facial recognition system and to inform decisions about Government investment and upgrades.

The Government could require law enforcement organisations to take further specific actions to understand how biometric technologies work and to mitigate any potential bias, both before they use them and while they use them. These could include testing requirements or rules about how the technology should be operated. Following appropriate consultation, the new oversight body would set these rules, potentially through a statutory code approved by Parliament. They could also check on compliance with these rules.

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?

Agree	Neither agree nor disagree	Disagree	Don't know

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.*

Answer:

About you

Please use this section to tell us about yourself

Full name	
Job title or capacity in which you are responding to this consultation exercise (for example, member of the public)	
Date	
Company name/organisation (if applicable)	
Address	
Postcode	
If you would like us to acknowledge receipt of your response, please tick this box	☐ (please tick box)
Address to which the acknowledgement should be sent, if different from above	

If you are a representative of a group, please tell us the name of the group and give a summary of the people or organisations that you represent.

Contact details and how to respond

Please send your response by 12/02/2026 to:

Data & Identity Directorate

2 Marsham Street, 1st Floor, Peel Building, London, SW1P 4DF

Email: fr-consultation@homeoffice.gov.uk

Complaints or comments

If you have any complaints or comments about the consultation process you should contact the Home Office at the above address.

Extra copies

Further paper copies of this consultation can be obtained from the above address, and it is also available online at <https://www.gov.uk/government/consultations/legal-framework-for-using-facial-recognition-in-law-enforcement>

Alternative format versions of this publication can be requested from fr-consultation@homeoffice.gov.uk

Publication of response

A paper summarising the responses to this consultation will be published on Gov.uk.

Representative groups

Representative groups are asked to give a summary of the people and organisations they represent when they respond.

Confidentiality

Information provided in response to this consultation, including personal information, may be published or disclosed in accordance with the access to information regimes (these are primarily the Freedom of Information Act 2000 (FOIA), the Data Protection Act 2018 (DPA), the General Data Protection Regulation (GDPR) and the Environmental Information Regulations 2004).

If you want the information that you provide to be treated as confidential, please be aware that, under the FOIA, there is a statutory Code of Practice with which public authorities must comply and which deals, amongst other things, with obligations of confidence. In

view of this it would be helpful if you could explain to us why you regard the information you have provided as confidential. If we receive a request for disclosure of the information we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding on the Home Office.

The Home Office will process your personal data in accordance with the DPA and in the majority of circumstances, this will mean that your personal data will not be disclosed to third parties.

Consultation principles

The principles that government departments and other public bodies should adopt for engaging stakeholders when developing policy and legislation are set out in the consultation principles.

<https://www.gov.uk/government/publications/consultation-principles-guidance>

Consultation principles, disclosure of responses and data protection principles that government departments and other public bodies should adopt for engaging stakeholders when developing policy and legislation are set out in the consultation principles. These can be found here: <https://www.gov.uk/government/publications/consultation-principlesguidance>

The Home Office, 2 Marsham Street, London, SW1P 4DF, is the data controller in respect of any information you provide in your answers. Your personal data is being collected and processed by the Home Office on the basis of informed consent. We will hold the data you provide for a maximum of 2 years. Further information can be found within the Government's Home Office Personal Information Charter. We will process the names and addresses, and email addresses provided by respondents, and information about which organisations respondents belong to, where this is provided. We will also process the information that you provide in relation to your responses. When the consultation ends, we will publish a summary of the key points raised on the Home Office website. This will include a list of the organisations that responded, but not any individual's personal name, address, or other contact details. All responses and personal data will be processed in compliance with the Data Protection Act 2018 and the UK General Data Protection Regulation. If you want some or all of the information you provide to be treated as confidential, it would be helpful if you could clearly identify the relevant information and explain why you consider it confidential in your response. Please note that we may be required by law to publish or disclose information provided in response to this consultation in accordance with the access to information regimes: primarily the Freedom of Information Act 2000 and the Data Protection Act 2018 and the UK General Data Protection Regulation. If we receive any request to disclose this information, we will take full account of your explanation but cannot give you an absolute assurance that disclosure will not be made in any case. We will not regard an automatic disclaimer generated by your IT system as a relevant request for these purposes. Once you have submitted your response to the consultation you will not be able to withdraw your answers from the analysis stage. However, under the Data Protection Act 2018 (and the UK General Data Protection Regulation), you have certain rights to access your personal data, and have it corrected or erased (in certain circumstances), and you can withdraw your consent to us processing your personal data at any time. You have the right to lodge a complaint to the Information Commissioner's Office about our practices, to do so please visit the Information Commissioner's Office website or contact the Information Commissioner at casework@ico.org.uk or: 18 Information Commissioner's Office Wycliffe House Water

Lane Wilmslow Cheshire SK9 5AF Telephone: 0303 123 1113 Textphone: 01625 545860
Monday to Friday, 9am to 4:30pm



© Crown copyright 2025

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3

Where we have identified any third-party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at <https://www.gov.uk/government/consultations/legal-framework-for-using-facial-recognition-in-law-enforcement>

Any enquiries regarding this publication should be sent to us at fr-consultation@homeoffice.gov.uk.