LIBERTY

NEW LEGAL FRAMEWORK FOR LAW ENFORCEMENT USE OF BIOMETRICS, FACIAL RECOGNITION AND SIMILAR TECHNOLOGIES: GOVERNMENT CONSULTATION

FEBRUARY 2026

CONTENTS

LIBERTY

ABOUT LIBERTY

Liberty is an independent membership organisation, founded in 1934. We challenge injustice, defend freedom and campaign to make sure everyone in the UK is treated fairly. We are campaigners, lawyers and policy experts who work together to protect rights and hold the powerful to account.

Liberty provides policy responses to Government consultations on issues which have implications for human rights and civil liberties. We also submit evidence to Select Committees, inquiries and other policy fora, and undertake independent research.

INTRODUCTION

1. Liberty welcomes the opportunity to respond to this consultation on law enforcement use of biometrics, facial recognition and similar technologies. Liberty has worked on issues of policing, surveillance, privacy and biometrics throughout our history, most relevantly acting as solicitors for Ed Bridges who challenged South Wales Police's use of live facial recognition technology in the world's first legal challenge of the sort.[1]

2. It has now been more than five years since the Court of Appeal found that South Wales Police's use of facial recognition was in breach of privacy rights, data protection laws and equality laws. It is our contention that the guidance and mitigations put in place as a result of that ruling have been at the very best insufficient.

3. The use of facial recognition has been allowed to explode over the past five years without a dedicated legal framework, without adequate safeguards, without transparency or real oversight, and without the benefit of an informed conversation with the public about where lines should be drawn. The year that this consultation began also saw the expansion of live facial recognition to more police forces across the country, the Metropolitan Police doubling their deployments, the installation and operation of fixed cameras in Croydon, a major expansion in retrospective facial recognition, and a series of disturbing revelations about racial bias in the system, the inclusion of children on watchlists, and the opaque and unregulated use of this privacy-infringing technology. We welcome this consultation, but it is long overdue.

4. Our response engages with each question with a particular focus on facial recognition, providing our perspective on how a framework may best protect people's rights and guard against abuse, and factors that the Home Office should take into account in the formulation of their policy on this issue. We advocate for a model inspired by the EU AI Act, whereby the most intrusive manifestations of these technologies require the highest justification, with a constrained list of legitimate purposes laid out in legislation, independent authorisation and safeguards in place to mitigate the impact on people's privacy. We urge the Home Office to ensure that the new oversight body is clearly constituted, truly independent and transparent, adequately resourced, and granted the necessary powers to ensure compliance. The success of the new framework will rely on the strength of this new body.

5. We look forward to seeing what emerges in legislation and engaging constructively on the specifics of the proposals. However, we are disappointed that the consultation rests on an assumption of greater and greater use of these technologies, with the pledge to "ramp up" use

[1] *R (Bridges) v Chief Constable of South Wales Police* ([2020] EWCA Civ 1058). 2 September 2020.

accompanying the launch, and the recent announcement of 40 new vans in the policing white paper. It is a significant missed opportunity that the most fundamental question of whether these technologies should be used at all is not being addressed through this consultation.

WHICH TECHNOLOGIES SHOULD THE NEW FRAMEWORK APPLY TO?

Question 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?

Question 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?

Question 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)?

Question 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.

6. Liberty believes that the new legal framework should extend as far as possible, to cover all of the above categories of technologies, with some caveats set out below. Our starting point is that it would be a missed opportunity to fail to capture invasive surveillance technologies that give rise to the same human rights concerns as facial recognition because of the technological difference in their operation. If law enforcement intends to use these technologies, there should be a strong legal framework to govern them.

7. The framework should apply to live, retrospective and operator-initiated facial recognition technology. Liberty supports a model similar to that in the EU AI Act whereby real-time biometric technologies such as live facial recognition are as a baseline banned, with use only allowed on the basis of serious need and independent authorisation, as outlined below. Retrospective facial recognition use has exploded in recent years, with Liberty Investigates reporting that searches of the Police National Database (PND) almost doubled from 2023 to 2024.[2] With the presence on the PND of millions of unlawfully stored images of people never charged with an offence, and the expanding use of other databases (also to be covered below), strong safeguards are urgently needed.

8. Other biometric technologies such as gait and voice recognition may be used alongside or instead of facial recognition and engage the same rights, so need to be brought under the framework. Gait recognition for example can not only be operated when a face is covered, but also at a greater range than facial recognition.[3]

9. Object recognition technologies do not process biometric data in the same way as many of the other technologies being discussed, but there are significant concerns about their ability to track and monitor individuals. In December 2025, Liberty Investigates reported on police use of a new

[2] Daniel Boffey and Mark Willding, Live facial recognition cameras may become 'commonplace' as police use soars, *The Guardian*, 24 May 2025, https://www.theguardian.com/technology/2025/may/24/police-live-facial-recognition-cameras-england-and-wales.
[3] *Privacy International*, How gait recognition technology can be used at a protest, 5 May 2021, https://privacyinternational.org/explainer/4496/how-gait-recognition-technology-can-be-used-protest.

app which analyses data collected by automated number plate recognition (ANPR) cameras, using artificial intelligence to identify track routes to identify "suspicious" journeys and vehicles to be stopped.[4] A car's licence plate may not be biometric data but it does allow for a person to be identified and tracked, and so these technologies should come under the framework.

10. There are however some of these technologies that we would warn against being used at all. Emotion recognition and certain other inferential technologies are widely seen as unethical excursions into pseudoscience, often reflecting cultural biases and lacking scientific validity.[5] As Ada Lovelace Institute have warned, "scientific consensus does not support the idea that complex emotional or psychological states can be reliably inferred from physical traits, especially across diverse populations", and these systems tend to reinforce harmful stereotypes relating to neurodivergence, cultural difference and disability, while operating without transparency or recourse.[6]

11. Article 5 EU AI Act lays out certain systems and practices that produce an unacceptable risk and so are prohibited from being placed on the market or put into service. These include AI systems for 'social scoring', predictive policing, the creation or expansion of facial recognition databases through the untargeted scraping of images from the internet or CCTV, biometric categorisation based on sensitive characteristics, emotion recognition in the workplace and schools, and AI systems that manipulate human behaviour or exploit people's vulnerabilities.

12. There is a strong argument for outright banning these and other technologies, such as emotion recognition systems more broadly, and Liberty would support this in principle. If they are not banned, the cleanest way to address this issue may be a technology-blind approach whereby the new body sets requirements relating to scientific validity, impact on rights, discriminatory effects and other factors, and does not allow any biometric, inferential or object recognition tools into use that cannot satisfy these requirements, whether they purport to read emotions, truth or faces. If the body is properly resourced and granted the necessary powers, this may better allow it to assess new and potentially concerning technologies as they emerge.

WHICH ORGANISATIONS SHOULD THE NEW FRAMEWORK APPLY TO?

Question 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?

13. Restricting the new legal framework solely to law enforcement organisations' use of facial recognition and similar technologies for a law enforcement purpose would be a missed opportunity. Liberty acknowledges the difficulty in drawing a precise line in this murky area but believes that the framework must apply as broadly as possible within the public sector and must capture any interaction with law enforcement.

[4] Mark Wilding & Charles Hymas, Police Given AI Tech to Track 'Suspicious' Car Journeys, *Liberty Investigates*, 15 December 2025, https://libertyinvestigates.org.uk/articles/police-ai-anpr-track-drivers.
[5] See for example: Mel Andrews, Andrew Smart & Abeba Birhane, The reanimation of pseudoscience in machine learning and its ethical repercussions, Patterns, 13 September 2024; ARTICLE 19, Emotional Entanglement: China's emotion recognition market and its implications for human rights, November 2020; Lisa Feldman Barrett, Ralph Adolphs, Stacy Marsella, Aleix M. Martinez and Seth D. Pollak, Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements, Psychological Science in the Public Interest, Vol. 20(I) 1-68, 2019.
[6] Nuala Polo & Jacob Ohrvik-Stott, An eye on the future: A legal framework for the governance of biometric technologies in the UK, *Ada Lovelace Institute*, May 2025, p.25, https://www.adalovelaceinstitute.org/wp-content/uploads/pdfs/30965/an-eye-on-the-future.pdf.

14. As facial recognition technology has become more accessible over time, its use has expanded not just in a specifically policing context, but by public bodies, local authorities, public transport and across the private sector as well. This has led to a confused environment with cameras owned and operated by different actors potentially having the same impact on people's rights from different angles. Trying to neatly cut law enforcement out of this picture for regulation under the framework, while leaving the others as they are, will just fuel this confusion.

15. As an illustration, in November 2025 the British Transport Police (BTP) announced that it would be trialling the use of live facial recognition technology at railway stations in London.[7] The consultation specifically names the BTP as a 'law enforcement agency' that would come under the framework, in a way that seems clear. Also last year, however, a representative of Transport for London (TfL) told the London Assembly Transport Committee that TfL were considering deploying facial recognition to "tackle fare evasion, and other more serious forms of criminality",[8] and Network Rail has tested various AI-enabled technologies including emotion recognition and object recognition at train stations since at least 2022.[9] Add in to this local authority cameras, any police deployments outside the station, and any private retail use on the concourse and the difficulty and drawbacks of drawing a clean division are clear.

16. In September 2025, Hammersmith and Fulham Council announced plans to invest £3.2 million on surveillance technologies including live facial recognition cameras, enhanced artificial intelligence capability for 500 existing cameras to enable retrospective facial recognition across the network, speakers and spotlights to be installed at camera sites, and even AI-enabled drones.

17. The Hammersmith and Fulham Council document explaining their facial recognition plans makes clear the false distinction being drawn in the consultation document between law enforcement and other actors, as it states "the use of facial recognition will require the support and cooperation of the Police to identify and take action against those responsible for perpetrating crime and anti-social behaviour in the borough".[10] The document goes on to emphasise this, stating "the scheme cannot and does not operate without a police support team".[11] Even in cases where the involvement of the police is less plainly stated than in Hammersmith and Fulham's proposal, if local authorities are to operate their own cameras, it is surely necessary that they be covered by the framework.

18. If the construction of 'law enforcement organisations' is inadequate for the framework, so too is 'for a law enforcement purpose'. The consultation paper cites s.31 Data Protection Act 2018, which lists the prevention, investigation, detection and prosecution of criminal offences, execution of criminal penalties, and safeguarding against and prevention of threats to public security. This would appear to exclude some of the purposes for which facial recognition is used (e.g. the search for missing people) and make the status of other applications such as the recent

[7] *British Transport Police*, British Transport Police to trial use of Live Facial Recognition technology, 26 November 2025, https://www.btp.police.uk/news/btp/news/england/british-transport-police-to-trial-use-of-live-facial-recognition-technology.
[8] Ross Lydall, Tube fare dodging: live facial recognition cameras could be used to catch most prolific evaders, *Evening Standard*, 9 July 2025, https://www.standard.co.uk/news/transport/facial-recognition-cameras-fare-dodging-tube-london-underground-tfl-b1237049.html.
[9] Matt Burgess, Amazon-Powered AI Cameras Used to Detect Emotions of Unwitting UK Train Passengers, *Wired*, 17 June 2024, https://www.wired.com/story/amazon-ai-cameras-emotions-uk-train-passengers.
[10] *London Borough of Hammersmith & Fulham*, CCTV and Artificial Intelligence – new innovations and improved infrastructure to help combat crime and anti-social behaviour, 15 September 2025, https://democracy.lbhf.gov.uk/documents/s132480/CCTV%20and%20Artificial%20Intelligence.pdf
[11] Ibid, para 13.

trials at the UK border somewhat unclear.[12] If one of the main purposes of introducing this new legal framework is to clarify and simplify the legal situation of the use of these technologies, we must not add further confusion by drawing lines in the wrong places.

19. While we do not currently call for the framework to cover private companies such as retail businesses, wherever there is interaction with law enforcement as the result of facial recognition use of any sort the framework should cover it. While something separate may be more appropriate for the governance of a private company's use of facial recognition, whatever stems from it for law enforcement purposes must be treated in the same way as if it had come from a law enforcement organisation.

HOW SHOULD THE FRAMEWORK PROTECT PEOPLE'S PRIVACY?

Question 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?

20. It is common ground that facial recognition interferes with the right to privacy. As a qualified right, it is possible for public authorities to interfere with the right to privacy, but for any interference to be justified, it must be in accordance with the law, in pursuit of a legitimate aim and necessary in a democratic society. However, necessity is not the same thing as utility, and if a tool is useful in pursuit of the legitimate aim of preventing crime and securing public order, that is not in itself enough to justify the interference.

21. As the European Court observed in *S and Marper v the United Kingdom*, a landmark case in which Liberty intervened relating to the handling of biometric data in the form of DNA, "the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private life interests".[13]

22. The factors listed in the consultation paper that the Government believes need taking into account in assessing whether the interference with privacy is justified are broadly good ones that we would agree with: seriousness of harm, purpose, consent, handling of data, who is impacted, and why. We believe that there are some important aspects that either are not covered or need to be drawn out in more detail, both to aid in assessing whether the interference is justified and also more broadly to help minimise the interference.

Necessity

23. Is using facial recognition technology and other biometrics strictly necessary in a given situation, or could other alternatives have been used instead? In *Glukhin v Russia*, the European Court highlighted the "highly intrusive" nature of facial recognition technology, emphasising that a "high level of justification" was required for facial recognition use to be deemed necessary in a

[12] Masha Borak, UK completes passport-free border trial with biometric e-gates, *Biometric Update*, 12 November 2025, https://www.biometricupdate.com/202511/uk-completes-passport-free-border-trial-with-biometric-e-gates; Elizabeth Greenberg, Live Facial Recognition to be Trialled at UK Border, *Digit News*, 10 November 2025, https://www.digit.fyi/live-facial-recognition-to-be-trialled-at-uk-border.

[13] *S and Marper v the United Kingdom*, Judgment, ECtHR, App. Nos. 30562/ 04 and 30566/04, 4 December 2008, para. 112.

democratic society, with "the highest level of justification required for the use of live facial recognition technology".[14]

24. Considering the highly intrusive nature of these technologies, authorisation to use them should be a meaningful process with a high bar to clear before they are used. A requirement to have an independent body assess requests for their use – including the factors raised in this section – seems an appropriate recognition of the seriousness of the interference with rights that they bring about.

Consent and notice

25. The current system of advanced notice informing the public of live facial recognition deployments is insufficient and does not give people enough of an opportunity to make an informed decision of whether they consent to be captured by the camera's scope or not. The College of Policing's Authorised Professional Practice (APP) document on facial recognition states that "forces should, unless in cases of critical threat when there is insufficient time, notify the public in advance of the deployment without undermining the objectives of the deployment. Details of the LFR are to be notified to the public using force websites and other appropriate communication channels (including social media)".[15] In practice, this takes the form of a social media post from a police force on the morning of a deployment, to be seen by few people and likely after a deployment has started.[16]

26. Advanced notice could and should be significantly strengthened, for example with a requirement to publish 14 days before a deployment (with an exception for urgent circumstances), publication not only on the website and social media but also on a centralised register cataloguing all police use of facial recognition technology, and a physical notice to be displayed at the site where the deployment is to take place. This would allow for effective monitoring, and enhance public confidence.

27. Where deployments are in progress, the APP states that "signs (or other equivalent awareness-raising measures) that publicise the use of the technology should be used to inform individuals in advance of their entering the zone of recognition. This measure is to alert members of the public to the presence of LFR technology and to allow them sufficient time to exercise their right not to walk into the zone of recognition". A code of practice issued by the new body should seek to ensure that these signs are displayed prominently enough outside of the range of the cameras that people are able to avoid them if they so wish, and it should be made very clear that avoiding cameras will not be taken as a reason for suspicion.

Watchlists

28. Watchlists for live facial recognition deployments should be bespoke, targeted, limited and transparent, based upon intelligence with the reasonable expectation that the people sought may be in the location targeted, and be made up of people whose offence justifies inclusion (as covered below). There should be a far higher bar for inclusion of children and other vulnerable people on a watchlist, with a restriction to safeguarding concerns and serious risk of harm seeming appropriate.

[14] *Glukhin v Russia* App. No. 11519/20, 4 July 2023, para 86-88.
[15] *College of Policing*, Live facial recognition: Authorised Professional Practice, 22 March 2022, https://www.college.police.uk/app/live-facial-recognition/where-date-time-duration-and-location-deployment.
[16] For example, this post on X (formerly Twitter) by Croydon MPS announcing a deployment to take place that day https://x.com/MPSCroydon/status/2019697576530923776. Accessed two days after it was posted, it had been 'viewed' only 350 times.

29. In 2025, every live facial recognition deployment by the Metropolitan Police operated with a watchlist between 14,919 and 16,883 people.[17] Reports of deployments so far in 2026 show all but one operating with between 16,834 and 16,966 people on the watchlist.[18] There is almost no variation whether a deployment takes place in Woolwich or Wembley, and these lists are large and growing. The average Metropolitan Police watchlist size for the ten deployments for which we have figures so far in 2026 is almost 2,000 higher than the average for the first ten deployments of 2025.

30. It is often difficult to find out who is on these lists and why. In December, Liberty Investigates found that hundreds of children as young as 12 have been included on watchlists for deployments.[19] The police were not able to say exactly how many children had been included, or provide the reasons that they appeared on these lists. In response, the Children's Commissioner said she was "deeply concerned" and that the revelation "raises serious questions about why this is needed and how it is being used".[20] While the APP states that there should be a "particular focus on ensuring the necessity case is fully made out" when children appear on watchlists, the Joint Committee on Human Rights have pointed out that the sheer number of times that children have been included "may indicate that insufficient care is being taken".[21]

31. In response to Liberty Investigates' reporting, the Information Commissioner's Office said, "Police must ensure deployments comply with the law, protect children's privacy, and have a clear rationale for including any individual on a watchlist".[22] The police have not managed to demonstrate their compliance with these factors. If the public are to have confidence in the new framework, it must be made clear how and when their children may come into contact with this technology, what specific safeguards will be in place to protect their privacy, and what the specific nature of the oversight will be to ensure that these interactions are rare, necessary and restricted to the fullest extent possible.

Location of deployments

32. Where deployments are held is an important factor that gives rise to several other potential issues. Questions of discrimination may arise for example if areas with a high minoritised population are targeted more than others, while deployments in the vicinity of schools may require greater justification in relation to the higher proportion of children expected to be captured by the cameras. Wherever deployments are held, attention must be paid to the potential cumulative impact of facial recognition use in a given area. A community being repeatedly targeted may have negative effects on cohesion and trust in the police.

33. Within a given area, the specific placement of the cameras must also give people the opportunity to avoid them. This does not just come down to signage and prior notification but where the

[17] *Metropolitan Police*, MPS LFR deployments, 2025, https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/deployment-records/live-facial-recognition-deployment-record-2025.pdf.
[18] The exception was a deployment in Croydon on 9 January which had a watchlist of 17,909. It is unclear why it was so large, although it is perhaps relevant that this deployment had the only reported false positive in the Metropolitan Police's log of deployments for the year (at time of writing showing up to 16 January). https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/live-facial-recognition-deployment-record-2026-to-date.pdf.
[19] Mark Wilding and Matt Dathan, Police forces use facial recognition to track children as young as 12, *Liberty Investigates*, 1 December 2025, https://libertyinvestigates.org.uk/articles/police-facial-recognition-children-met-government-consultation.
[20] Ibid.
[21] Joint Committee on Human Rights, Letter to the Secretary of State for the Home Department, 18 December 2025, https://committees.parliament.uk/publications/50866/documents/281535/default/.
[22] Wilding and Dathan, Police forces use facial recognition to track children as young as 12, *Liberty Investigates*.

cameras themselves are. If people are told that they are allowed to avoid a camera, but there is no other way to get to an essential location such as a hospital, school, a place of worship – or indeed a protest – this is not meaningful consent. These are all places where there would be a higher than normal expectation of privacy, and guidelines around the use of facial recognition should respect that.

Data and source images

34. While Liberty is critical of law enforcement use of facial recognition technology, we acknowledge that there are some areas of good practice, such with the instantaneous deletion of data that does not produce a match. This should be reflected in the framework so that the good practice becomes a legal requirement.

35. Other aspects of data handling and the sourcing of images are of greater concern. Where an image has been taken from should always be a consideration in assessing the interference with privacy of a use of facial recognition. Images that originate from within law enforcement such as custody images will generally be more acceptable than those that originate externally, e.g. from social media, smart doorbells and CCTV, which should require a higher level of justification. The untargeted scraping of facial images from the internet or CCTV footage for the purpose of creating or expanding facial recognition databases is prohibited under the EU AI Act, and this should be mirrored in the new framework.[23]

36. May 2024, Liberty Investigates revealed that Metropolitan Police computers had accessed the PimEyes private facial recognition tool 2,337 times in just three months.[24] We can see no justification for the use of this sort of third party tool, and would advocate that this use is banned also. We will cover the searching of other databases below.

HOW SHOULD THE FRAMEWORK PROTECT OTHER RIGHTS?

Question 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?

37. The consultation is right to point out that facial recognition technology interferes with other rights beyond the right to privacy, most notably the prohibition on discrimination, which will be covered below in questions 16 and 17. We are however concerned about the implication of this question, suggesting that there is a "balanced way" in which to use facial recognition at protests. The impact on the right to freedom of expression and freedom of assembly of using facial recognition technology at protests is too great to justify any use.

38. The rights to freedom of expression and assembly are important not only in themselves, but also as enabling rights that allow societies to ensure the peaceful enjoyment of their other rights as well. As the UN Human Rights Committee put it, freedom of assembly "constitutes the very foundation of a system of participatory governance based on democracy, human rights, the rule

[23] Article 5(1)(e).
[24] Mark Wilding and Cahal Milmo, Met Police computers access 'dangerous' facial recognition search engine, *Liberty Investigates*, 10 May 2024, https://libertyinvestigates.org.uk/articles/met-police-computers-access-dangerous-facial-recognition-search-engine.

of law and pluralism".[25] Freedom of assembly is a positive right, requiring authorities to actively facilitate its exercise. We believe that the use of facial recognition could have the opposite effect.

39. Participating in a protest by its very nature involves associating oneself with a particular political position, group or cause. As the goal is generally to influence those in power to adopt or abandon a policy, this will often place the protester in the role of opponent or dissident. Participants have a legitimate expectation of anonymity unless their conduct presents reasonable grounds for arrest and, there are often good reasons for wanting this anonymity to be preserved. Even outside of the context of protest, in 2019 the London Policing Ethics Panel found that 38% of people aged 16-24 would stay away from events where they knew LFR would be used.[26] The 'chilling effect' of facial recognition is concerning no matter where it is deployed. In the context of protest, it is intolerable.

40. In 2024, the United Nations published a 'practical toolkit for law enforcement officials to promote and protect human rights in the context of peaceful protests'. It states "Digital technologies should not be used to categorize, profile or remotely identify individuals, including by biometric means, before, during, or after protests. The use of such technologies at protests is inconsistent with the obligation to facilitate the right to peaceful assembly".[27] Liberty agrees, and believes that this should be a red line in the new legal framework.

FOR WHAT PURPOSE SHOULD LAW ENFORCEMENT ORGANISATIONS BE ALLOWED TO USE THESE TECHNOLOGIES?

Question 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?

Question 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.

41. Liberty believes that the provisions set out in the EU AI Act generally strike the right balance between protecting the rights of the public and enabling the extraordinary use of these invasive biometric technologies for a policing purpose where there is genuine need. At present, facial recognition is used for a wide variety of reasons, often targeting people wanted for very low-level offences. Liberty believes there should be a higher bar.

42. Article 5(1)(h) EU AI Act prohibits generally the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement. Live facial recognition

[25] *UN Human Rights Committee*, General Comment No. 37, 2020, https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-37-article-21-right-peaceful.
[26] *London Policing Ethics Panel*, Final Report on Live Facial Recognition, May 2019, p. 24, http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/live_facial_recognition_final_report_may_2019.pdf.
[27] *United Nations Office of the High Commissioner for Human Rights*, Practical toolkit for law enforcement officials to promote and protect human rights in the context of peaceful protests, 7 March 2024, para 16, https://www.ohchr.org/en/documents/tools-and-resources/practical-toolkit-law-enforcement-officials-promote-and-protect-human.

deployments can however take place (with authorisation, as discussed below), where it is strictly necessary for one of the following objectives:

a) the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons;

b) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack;

c) the localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years.

43. These offences, listed in the Annex, are as follows: terrorism, trafficking in human beings, sexual exploitation of children, and child pornography, illicit trafficking in narcotic drugs or psychotropic substances, illicit trafficking in weapons, munitions or explosives, murder, grievous bodily injury, illicit trade in human organs or tissue, illicit trafficking in nuclear or radioactive materials, kidnapping, illegal restraint or hostage-taking, crimes within the jurisdiction of the International Criminal Court, unlawful seizure of aircraft or ships, rape, environmental crime, organised or armed robbery, sabotage, and participation in a criminal organisation involved in one or more of the offences listed above.

44. This high bar set out in the EU AI Act is commensurate with the high level of intrusion and interference with people's rights inherent in live facial recognition, as recognised by the European Court of Human Rights in *Glukhin v Russia*. Using this powerful and invasive technology on low-level offences is disproportionate and should not be allowed.

45. For the use of retrospective facial recognition, we consider that it is appropriate to set a lower bar of seriousness than should be required for the use of live facial recognition. Setting this at the level of a 'qualifying offence' as listed in s65 Police and Criminal Evidence Act 1984 would neatly align the threshold for the use of retrospective facial recognition with that of retention of DNA profiles and fingerprints.[28]

WHO SHOULD DECIDE WHEN LAW ENFORCEMENT ORGANISATIONS CAN USE TECHNOLOGIES LIKE FACIAL RECOGNITION?

Question 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.

[28] See: *Home Office*, Protection of Freedoms Act 2012: DNA and fingerprint provisions, 4 February 2019, https://www.gov.uk/government/publications/protection-of-freedoms-act-2012-dna-and-fingerprint-provisions--2/protection-of-freedoms-act-2012-dna-and-fingerprint-provisions-january-2019.

Question 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.

46. Liberty agrees that some uses of facial recognition and similar technologies require more senior authorisation, and there are circumstances where this authorisation should come from an independent authority. Reflecting the treatment of this question in the EU AI Act, we believe that all uses of live facial recognition should require independent authorisation. We recognise that this is not feasible for retrospective facial recognition.

47. Article 5(3) EU AI Act states that any use of live facial recognition by law enforcement shall be subject to a "prior authorisation granted by a judicial authority or an independent administrative authority whose decision is binding of the Member State in which the use is to take place, issued upon a reasoned request and in accordance with the detailed rules of national law". The Act does also make provision that in a "duly justified situation of urgency", a deployment may be commenced without authorisation, provided that it is requested "without undue delay, at the latest within 24 hours" and immediately stopped if authorisation is not granted. We consider that this strikes a reasonable balance.

48. Requirements for independent authorisation or warrants are not uncommon in related contexts in law enforcement, for example under the Intelligence Services Act 1994, Police Act 1997, and Investigatory Powers Act 2016. The Investigatory Powers Act (IPA) requires in particularly intrusive contexts a 'double lock' of authorisation whereby a warrant is approved by both the Secretary of State and a Judicial Commissioner.

49. Judicial Commissioners must have regard to the tests of proportionality and necessity as applicable under the Human Rights Act 1998, and to the general privacy duties set out in s.2 IPA, in particular whether what is sought by the authorisation could reasonably be achieved by other means, whether the level of protection to be applied is higher due to the particular sensitivity of that information, the public interest in the integrity and security of telecommunication systems and postal services, and any other aspects of the public interest in the protection of privacy. Other sections in IPA provide additional safeguards for matters such as legal professional privilege and journalistic material and sources.[29]

50. If the purpose of this consultation is to provide for an environment in which the use of facial recognition technology is made available to the police in a way that respects people's rights, enhances transparency and meaningful oversight, and fosters confidence and certainty in the public and law enforcement alike, a strictly circumscribed set of legitimate purposes coupled with a requirement for independent authorisation appears to us the best way of achieving it. These provisions are already in place in the EU and in certain forms in UK legislation, and should be considered for inclusion in the new legal framework.

SHOULD LAW ENFORCEMENT ORGANISATIONS BE ALLOWED TO SEARCH OTHER PUBLIC RECORDS WITH THIS TECHNOLOGY?

Question 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

[29] Sections 26-29, 111-114, and Part 6.

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?

Question 13: If biometric searches of other government databases take place, what safeguards should be in place?

51. Liberty opposes the use of public records such as the passport, immigration and driving licence databases for the purpose of facial recognition searches. The millions of photographs of law-abiding members of the public on these databases were submitted to enable them to prove their identity, travel across borders, drive a car, demonstrate their immigration status, or another specific reason. They were never intended to act as a digital identity parade, and nor was it a reasonable assumption that they would end up being so.

52. This distinguishes them from law enforcement-specific databases, most notably the Police National Database (PND), populated by custody images. Here there is a reasonable expectation and policing justification that the images may be repurposed for facial recognition use. Even here there is the very serious caveat that custody images of people arrested but never charged with any crime remain on the PND, almost a decade and a half after they were supposed to be deleted.[30]

53. Much of what the public know about the use of other databases for facial recognition searches comes from freedom of information requests and investigative reporting, including by Liberty Investigates. In January 2024, Liberty Investigates revealed that police forces had been secretly conducting facial recognition searches on the passport database since at least 2019.[31]

54. In May 2025, Liberty Investigates reporting further revealed that more than a thousand searches had been conducted on the passport database in the two years previous, with 110 searches of the immigration database made in 2024 as well. Liberty Investigates found that officials had concluded that using the passport database was "not high risk" and "not controversial", according to internal documents, and that the department had not sought advice from the Information Commissioner.[32] Both the nature of these revelations and the fact that they had to be extracted by investigative journalists are seriously concerning.

55. The consultation paper suggests that biometric searches of other Government databases may be permitted for 'serious' offences, for a safeguarding purpose, and/or to identify injured, unwell or deceased people. Together, this does not constitute a high enough bar and would seem to lead to searches of these databases becoming routine. If these searches are to take place, they must be on the basis of extraordinary need that recognises the engagement with the rights of millions of unaware people.

56. The suggested safeguards in the paper are approval of search requests by a senior police officer or independent body, and search records kept for review again by a senior police officer or independent body. We do not believe that searches of these other databases should be happening at all, but if they are then the involvement and oversight of an independent body as

[30] James Meikle, Police may have to destroy photos of innocent people after court ruling, *The Guardian*, 22 June 2012, https://www.theguardian.com/uk/2012/jun/22/police-photos-innocent-court-ruling .
[31] Mark Wilding and Charles Hymas, Police secretly conducting facial recognition searches of passport database, *Liberty Investigates*, 8 January 2024, https://libertyinvestigates.org.uk/articles/police-secretly-conducting-facial-recognition-searches-of-passport-database.
[32] Mark Wilding and Daniel Boffey, Live facial recognition cameras may become 'commonplace' as police use soars, *Liberty Investigates*, 24 May 2025, https://libertyinvestigates.org.uk/articles/uk-police-forces-pursuing-major-expansion-of-facial-recognition-capabilities.

opposed to a policing figure is necessary, along with strict transparency requirements and searches conducted only in relation to the most serious offences.

WHO SHOULD MAKE SURE LAW ENFORCEMENT ORGANISATIONS ARE USING THIS TECHNOLOGY RESPONSIBLY?

Question 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).

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

57. Designing a strong and effective oversight body is vital, as it is this on which the success of the new framework will rely. Liberty is in favour of the newly constituted oversight body having each of the powers and obligations listed in the consultation document, and going further as well to make provision relating to procurement, testing and scientific validity, and reporting requirements.

58. In considering what makes an effective oversight body, Liberty enlisted the support of our partners in the International Network of Civil Liberties Organisations (INCLO), a worldwide network of 15 prominent national civil liberties and human rights organisations.[33] INCLO analysed nine oversight bodies across eight jurisdictions to assess what factors help to produce an effective authority. The following bodies were considered:

    - Court of Audit, Belgium
    - National Audit Office (Riigikontroll), Estonia
    - European Data Protection Supervisor (EDPS), European Union
    - Commission Nationale de l'Informatique et des Libertés (CNIL), France
    - Independent Commission Against Corruption (ICAC), Hong Kong
    - Independent Policing Oversight Authority (IPOA), Kenya
    - Office of the Auditor-General (OAG), New Zealand
    - Federal Trade Commission (FTC), United States
    - Government Accountability Office (GAO), United States.

59. While they each have different remits and focuses from each other and the proposed new body, a number of factors emerged that can be considered important in ensuring meaningful oversight of this new legal framework.

[33] INCLO's 15 member organisations are the American Civil Liberties Union (ACLU); the Association for Civil Rights in Israel (ACRI); the Canadian Civil Liberties Association (CCLA); the Centro de Estudios Legales y Sociales (CELS) in Argentina; Dejusticia in Colombia; the Egyptian Initiative for Personal Rights (EIPR); the Human Rights Law Network (HRLN) in India; Human Rights Law Centre (HRLC) in Australia, the Hungarian Civil Liberties Union (HCLU); the International Human Rights Group Agora (Agora) in Russia; the Irish Council for Civil Liberties (ICCL); the Kenya Human Rights Commission (KHRC); KontraS in Indonesia, the Legal Resources Centre (LRC) in South Africa; and Liberty in the United Kingdom.

Clear legal or constitutional mandates establishing powers and scope.

60. A clear establishing mandate gives an oversight body necessary legitimacy and a strong legal basis for its actions, while ensuring that its remit is widely understood, enhancing certainty and accountability. In some cases this stems directly from the country's constitution (such as with the Court of Audit in Belgium) or fulfils a constitutional role (in the case of the Kenyan IPOA). Elsewhere, clear legislation such as Estonia's National Audit Act establishes the body's legal authority and what is expected from the entities it has power over. We would urge the Home Office to lay out as clearly as possible the powers and scope of the new body in primary legislation.

Independence in appointment and operation, often involving multiple branches of government or fixed terms.

61. The new body will not work unless it both is and is seen to be independent. Different bodies in different jurisdictions achieve this in different ways. In the European Union, Regulation (EU) 2018/1725 explicitly provides for the institutional independence of the EDPS, requiring it to act with complete independence, free from external instructions, and maintain professional confidentiality, while in Kenya the IPOA Act insists that the body, in performing its functions, "shall not be subject to any person, office, or authority," and no one may interfere with its decision-making or operations.

62. In New Zealand, the Public Audit Act obliges the Auditor-General to act independently in exercising all functions, duties, and powers, and the OAG explicitly cannot be directed by the Government or Parliament on what to audit or prioritise. Appointments to these bodies are generally taken out of the (sole) hands of the executive, while fixed terms (such as served by the head of the GAO in the United States) allow for greater certainty as well as protecting the heads of these bodies from removal.

Adequate capacity, including technical expertise, staffing, and budget.

63. Any discussion of powers and functions for a new body will be entirely theoretical if it is not imbued with the capacity necessary to carry them out. Kenya's IPOA may have good enabling legislation, but significant resource constraints have seriously limited the Authority's capacity to handle complaints and operate effectively,[34] while on the other hand the capacity available to CNIL in France has allowed it to process more complaints than it received in 2024, despite receiving a record number.[35]

Power to publish findings and require follow-up actions or to compel compliance.

64. The exact nature of the powers given to these oversight bodies vary, and not all would be appropriate in this current context, but in all cases it is clear that some way of ensuring compliance is a necessary component of an oversight body. In Hong Kong, the ICAC has powers of investigation, search and arrest, alongside their functions of systemic reviews, preventative studies and offering guidance to institutions to promote broader compliance, while the FTC in the United States may bring administrative proceedings or seek injunctions to stop unlawful practices or products or pause transactions to allow for investigation to take place.

[34] *KBC Digital*, Lack of funding, police cooperation crippling IPOA oversight role, 31 August 2025, https://www.kbc.co.ke/lack-of-funding-police-cooperation-crippling-ipoa-oversight-role.
[35] *CNIL*, Annual report: CNIL's achievements and key actions in 2024, 29 April 2025, https://www.cnil.fr/en/annual-report-2024.

65. The EDPS conducts audits and investigations, issues guidance, and handles complaints to verify compliance in practice. It can issue warnings and reprimands, impose bans or administrative fines, and can refer matters to the Court of Justice of the EU for legal enforcement. Access for these bodies is often enforced. In Estonia, Riigikontroll's powers are supported by strong access rights to information, premises, assets, and documents, with obstruction treated as a reportable offense to Parliament, while in New Zealand, the OAG can examine individuals under oath where necessary.

Transparency and public reporting, strengthening accountability and public trust.

66. Ensuring transparency through public reporting is a key function of a successful oversight body, and an effective way of improving public confidence. Many of the bodies studied publish annual reports, such as with Belgium's Court of Audit, whose reports are submitted to legislative assemblies to inform parliamentary scrutiny. Effective, transparent reporting can also function as a form of public education, which is keenly needed in this area.

67. Further elaboration on the function of independent oversight bodies specifically in relation to facial recognition can be found in INCLO's report 'Eyes on the Watchers: Challenging the Rise of Police Facial Recognition'.[36]

HOW SHOULD THE NEW FRAMEWORK GUARD AGAINST BIAS AND DISCRIMINATION?

Question 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.

Question 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.

68. Liberty agrees that 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. This is clearly still a significant problem not being adequately addressed under the current system.

69. The contention that live facial recognition operated at the threshold in current use by police forces across the country is free from racial bias is problematic for three reasons. The first is that the study cited by the Metropolitan Police as evidence of this lack of bias has been criticised as "insufficient to support the claims being made".[37] The second is that false alerts continue to display considerable racial disproportionality. In the year to September 2025, the Metropolitan Police reported 10 false alerts from live facial recognition deployments, with 8 of the 10 people

[36] *INCLO*, Eyes on the Watchers: Challenging the Rise of Police Facial Recognition – Principles to reduce the human rights harms of facial recognition technology, 12 February 2025, https://inclo.net/wp-content/uploads/2024/03/INCLO-FRT-Principles-Final.pdf.
[37] Vikram Dodd, Expert rejects Met police claim that study backs bias-free live facial recognition use, *The Guardian*, 23 August 2025, https://www.theguardian.com/technology/2025/aug/23/expert-rejects-met-police-claim-that-study-backs-bias-free-live-facial-recognition-use.

wrongly identified being Black.[38] The third is that there is no law in place mandating that facial recognition is only used at a threshold deemed high enough to mitigate racial disproportionality.

70. With retrospective facial recognition, the situation is even more concerning. In December, the Home Office revealed that the retrospective facial recognition tool the police had been using to search the Police National Database was extremely racially disproportionate at certain settings, with false positive rates at 9.9% for Black women compared to 0.1% for white women. Reporting by Liberty Investigates found that the police not only knew about this, but actually successfully lobbied to use the biased settings.[39]

71. It is unknown what impact the use of this racially biased tool has had, and while we hope that the HMICFRS review will answer some questions, a properly resourced new oversight body should ensure that this does not ever happen again.

72. Some of the factors that the new body should consider in setting rules to guard against bias and discrimination should therefore include rigorous testing of the tools being used, setting of the thresholds at which they may be operated, justification for the choice of locations subject to facial recognition deployments, the impact assessments that must be required before use of the tools and the transparent reporting that must take place after.

73. Considering other technologies considered in the consultation, the oversight body should also take into account the potential racial and cultural factors that may affect the perceived results of inferential technologies and set guidelines around the application to object recognition technologies relating to cultural norms.

74. Across all of this, it should be recognised that bias and discrimination in facial recognition and related technologies is both a technological and a human question, and both sides of that equation must be addressed. As we have seen, it is one thing to set a particular threshold for facial recognition use, and another to ensure it is stuck to.

SUMMARY OF RECOMMENDATIONS

75. Liberty recommends:

- The new legal framework should extend as far as possible, to cover all of the technologies listed in the consultation.
- The framework should apply to all public sector use of facial recognition and similar technologies, and cover any interaction with law enforcement. Private sector use should be dealt with separately.
- Strong safeguards should be in place to protect people's privacy, including restrictions on watchlist composition, a strengthened system of advanced notice, guidance around location of deployments, and requirements relating to data handling and the sourcing of images.

[38] *Metropolitan Police*, Live Facial Recognition: Annual Report, September 2025, https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/other-lfr-documents/live-facial-recognition-annual-report-2025.pdf.
[39] Mark Wilding and Daniel Boffey, UK police forces lobbied to use biased facial recognition technology, *Liberty Investigates*, 10 December 2025, https://libertyinvestigates.org.uk/articles/police-forces-biased-facial-recognition-technology.

- Facial recognition should never be used at protests.
- Live facial recognition should be prohibited by default, with specified exceptions for the most serious crimes, substantial and imminent threat to life, and the targeted search for specific missing persons and victims of abduction and trafficking.
- Independent authorisation should be required for all uses of live facial recognition.
- Other databases should not be made available for facial recognition searches, except for in the most extreme circumstances and with the authorisation, oversight and reporting of an independent body.
- The new oversight body should be given a clear legal mandate establishing its powers and scope, be fully independent in its appointment and operation, have the necessary power to compel compliance, and be fully transparent with regular public reporting.
- The new body should set rules for law enforcement to follow to guard against bias and discrimination and check compliance with these rules. This should include testing the tools, setting thresholds, requiring impact assessments, and other factors.