Response to Government Consultation

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

Prof. Pete Fussey & Dr. Daragh Murray

10 February 2026

## Introduction

1. This submission is made by Prof. Pete Fussey,[1] University of Southampton, and Dr. Daragh Murray,[2] Queen Mary University of London. Both are internationally recognised experts with respect to the human rights impacts of new technologies, including facial recognition technology (FRT).
2. The authors conducted the only independent academic review of the Metropolitan Police's use of facial recognition technology,[3] published *Facial Recognition Technology: Policing and Human Rights in the Age of Artificial Intelligence* with Oxford University Press,[4] authored several peer-reviewed studies,[5] have contributed to authoring United Nations guidance in this area,[6] and led research for EU agencies on the use of remote biometric technologies in seven member states (forthcoming).
3. Before addressing the individual questions raised as part of the consultation, four overarching issues should be highlighted.
    - **Legislation should be restrictive, rather than permissive.** The circumstances in which FRT, or any other new technologies, may be used should be clearly demarcated, in order to limit the scope for discretion,[7] and to ensure compliance with the 'necessary in a democratic society'[8] requirement. It is equally important that the 'in accordance with the law'[9] requirement be respected. Common to other forms of intrusive surveillance technologies, an appropriate legal basis must regulate any law enforcement use of such technologies. In the absence of an

[1] Professor of Criminology and Head of Department, Department of Sociology, Social Policy and Criminology.

[2] Reader in International Law and Human Rights. The work underpinning this submission is supported by a UKRI Future Leaders Fellowship Grant M/T402133/3.

[3] Pete Fussey & Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology', Human Rights, Big Data & Technology Project, July 2019.

[4] Pete Fussey & Daragh Murray, *Facial Recognition Technology: Policing and Human Rights in the Age of Artificial Intelligence* (OUP, 2025).

[5] Fussey, P., Davies, B. and Innes, M. (2021) 'Assisted' Facial Recognition and the Reinvention of Suspicion and Discretion in Digital Policing. *The British Journal of Criminology* 61(2): 325-344; Daragh Murray, Police Use of Retrospective Facial Recognition Technology: A Step Change in Surveillance Capability Necessitating an Evolution of the Human Rights Law Framework (2023) Modern Law Review; Daragh Murray, Facial Recognition and the End of Human Rights As We Know Them? (2024) Netherlands Quarterly of Human Rights.

[6] See, e.g., Model Protocol for Law Enforcement Officials to Promote and Protect Human Rights in the Context of Peaceful Protests, UN Doc. A/HRC/55/60, 31 January 2024; UN Special Rapporteur on the Rights to Freedom of Assembly and of Association, Human rights compliant uses of digital technologies by law enforcement for the facilitation of peaceful protests, January 2024. Available at: https://www.ohchr.org/sites/default/files/2024-03/Toolkit-law-enforcement-Component-on-Digital-Technologies.pdf.

[7] This requirement was established by the Cout of Appeal in *Bridges*. See, *R (Bridges) v. The Chief Constable of South Wales Police* [2020] EWCA Civ 1058, paras. 91, 94.

[8] *Catt v. the United Kingdom*, Judgment, ECtHR, App. No. 43514/15. 24 January 2019, para. 106.

[9] *S and Marper v. the United Kingdom*, Grand Chamber, ECtHR, App. No. 30562/04, 30566/04, 4 December 2008, para. 95.

appropriate legal framework law enforcement should not be permitted to experiment on the public.[10]

- **There can be no 'one size fits all' approach to FRT or other biometric identification technologies.** Different use cases will give rise to (often significantly) different law enforcement benefits and harms to human rights.[11] Each use case must be addressed independently. A use case refers to the type of technology, application and purpose of use.
- **Evidence-based assessment of potential utility and potential harm are essential.** Resolving the 'competing interests'[12] at play requires evaluating the potential utility to law enforcement and the potential harm to human rights, of each use case. The determination of both utility and harm must be evidence-based and rely on accepted standards of evidence.[13] Given FRT's novelty and significant surveillance potential this is not a trivial task. This is, however, an obligation of the State.[14] To date, no concrete *evidence* justifying the need for live FRT has been presented. Peer reviewed evidence demonstrates that benefits are often assumed and harms routinely dismissed.[15] Moreover, many public justifications of FRT rely on research that, on analysis, does not substantiate the claims being made.[16]
- **This evidence should be subject to independent expert scrutiny to ensure appropriate levels of friction within the legislative process**.

**<u>Question 1: Neither Agree Nor Disagree</u>**

4. The decisive factor in responding to this question is whether the envisaged 'uses of biometric technologies' are necessary in a democratic society, or not.
5. As noted in the introduction, two considerations are particularly relevant.
6. First, a one size fits all approach to biometric technologies is inappropriate. The potential law enforcement benefit and the potential harm to human rights will differ significantly dependent upon which biometric technologies are selected and how they are deployed. Each use case – and its necessity in a democratic society – must therefore be evaluated on a case-by-case basis.

---

[10] Police use of FRT has, to-date, occurred absent an adequate legal framework. The resultant lack of transparency is problematic from a rule of law perspective. It is noted, for example, that every police constabulary in the UK has been using retrospective facial recognition technology for a number of years, despite repeated denials. See, Liberty Investigates, 'Hundreds of Thousands of Innocent People on Police Databases as Forces Expand Use of Facial Recognition', 25 September 2023.

[11] For instance, the use of FRT at a border post to identify travellers gives rise to significantly different human rights considerations than the use of FRT across public surveillance cameras to identity individuals suspected of having committed a crime.

[12] *S and Marper v. the United Kingdom*, Grand Chamber, ECtHR, App. No. 30562/04, 30566/04, 4 December 2008, para. 112.

[13] See Pete Fussey & Daragh Murray, *Facial Recognition Technology: Policing and Human Rights in the Age of Artificial Intelligence* (OUP, 2025), chapters 2 & 4.

[14] States are subject to an obligation 'to respect' human rights. See, Article 1, European Convention on Human Rights.

[15] See Fussey and Murray (2025) for analysis of assumed benefits attributed to FRT.

[16] A notable example concerns public claims that draw on a 2023 National Physical Laboratory study to variously claim that any bias on NEC's LFR algorithm does not exist at thresholds for operational use, or is not 'statistically significant', is a case in point. (See National Physical Laboratory. 2023. Facial Recognition Technology in Law Enforcement Equitability Study. Final Report, https://science.police.uk/site/assets/files/3396/frt-equitability-study_mar2023.pdf). This issue is analysed in detail in the peer-reviewed work of Fussey and Murray (2025), and a summary of key arguments was reported by The Guardian here: https://www.theguardian.com/technology/2025/aug/23/expert-rejects-met-police-claim-that-study-backs-bias-free-live-facial-recognition-use.

7. Second, the necessity calculation must be evidence-based. The potential utility and potential harm associated with each use case must be clearly established. The risks accompanying a blanket authorisation – i.e. overly permissive, rather than restrictive legislation – are that such important differences become overlooked and that new, more untested, variants of a technology are given tacit approval. Moreover, in the future, the category of 'biometric technologies' may encompass technologies that are yet to be anticipated. The adaptation of older legislation to new technology not only raises human rights concerns but, as peer-reviewed research has shown, creates obstacles for those responsible for providing public safety.[17]

**Question 2: Neither Agree Nor Disagree**

8. The same considerations raised in response to Question 1 apply.
9. With respect to the establishment of an appropriate evidence base justifying each use case, however, it is important to note that consistent attempts to deploy technologies to infer emotion and intent consistently have been dismissed as pseudo-science.[18] Equally, many claims and inferences drawn from a selection of high-profile biometric idenitification techniques routinely fail to achieve substantiation by appropriate evidence.[19]

**Question 3**

10. The same considerations raised in response to Question 1 apply.
11. Three additional considerations also arise.
12. First, there must be clarity as to when use of this technology becomes 'directed surveillance', bringing the Regulation of Investigatory Powers Act 2000 into play.
13. Second, if brought into new legislation, the circumstances in which this technology can be used must be appropriately delimited,[20] including with respect to how this technology may be used in combination with other surveillance or analytical tools.
14. Third, any use of such technologies in the context of protest must be in line with the Model Protocol for Law Enforcement Officials to Promote and Protect Human Rights in the Context of Peaceful Protest.[21] As noted in the toolkit accompanying the Protocol:

> Any use of digital technologies by law enforcement within the context of peaceful protests should be for the express purpose of facilitating the right to freedom of

[17] Fussey, P. and Sandhu, A. (2022) Surveillance Arbitration in the Era of Digital Policing. *Theoretical Criminology* 16(1): 3-22.

[18] Fussey and Murray (2025); Maguire, M. and Fussey, P. (2016) Sensing Evil. *Focaal: Journal of Global and Historical Anthropology* (75): 31-44; Maguire, M., and Fussey, P. (2026 IN PRESS) *The Empty Watchtower: Counterterrorism after 9/11*, New York: New York University Press

[19] See above and, in the case of Gait Analysis, the following authoritative sources challenged the scientific validity and overclaimed benefits of this method during its use within the criminal justice process: Forensic Science Regulator. (2019) Code of Practice for Forensic Gait Analysis. Available from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/918878/137_Forensic_Gait_Analysis_Issue_2.pdf; The Royal Society. (2017) *Forensic Gait Analysis: A primer for courts*. London: The Royal Society, available from https://royalsociety.org/-/media/about-us/programmes/science-and-law/royal-society-forensic-gait-analysis-primer-for-courts.pdf. Other feted 'innovations' in biometric identification including 'super-recognition' and sentiment analysis have received extensive criticism from the scientific community.

[20] Noting, for instance, the significant purpose different between using this technology in real-time in response to the commission of a crime, versus its use to monitor for intelligence purposes.

[21] Model Protocol for Law Enforcement Officials to Promote and Protect Human Rights in the Context of Peaceful Protests, UN Doc. A/HRC/55/60, 31 January 2024. See in particular paras. 61 and 62.

peaceful assembly and enabling and protecting other associated rights, such as the right to privacy and freedom of expression. The use of such technologies should be in accordance with a limiting principle to circumscribe their use, rather than an authorising principle that permits expansive use.[22]

**Question 4: Don't Know**

15. As noted, any legislation should be restrictive rather than permissive in order to ensure compliance with the necessary in a democratic society requirement.
16. It is important to recognise that options exist beyond flexible versus 'fresh' legislation. One solution could be to explore further the relationship between law and policy, such as the use of adaptive yet legally binding codes of practice to accommodate technological innovation. Variations of this approach have been highlighted in recent reviews of biometric surveillance and its oversight.[23]
17. Irrespective of whether new technology is addressed on the basis of flexible or fresh legislation two overarching considerations apply.
    - The case for inclusion of new technologies must be evidence-based, clearly setting out the potential benefit and potential harm to human rights of the new technology, in each use case.
    - This evidence must be subject to independent expert oversight, with the authority to reject the use of a new technology, or to circumscribe its use.

**Question 5: Agree**

18. Legislation should apply to all law enforcement *uses* of FRT or similar technologies. This must include law enforcement uses of data obtained, or analysed, by non-law enforcement actors. If law enforcement agencies establish a relationship with non-law enforcement actors, whether formal or informal, the whole process of data collection and use should be regulated in line with the obligations placed on law enforcement.

**Question 6**

19. As established in legal proceedings, FRT is an exceptionally intrusive surveillance capability and its use demands a 'high level' of justification.[24]
20. As repeatedly emphasised in this submission, necessity cannot be evaluated on a one size fits all basis. It is dependent upon the use case at hand.
21. Resolving the 'competing interests' at play is central to the necessity test. This is dependent upon an evidence-based evaluation of both potential utility and potential harm.

---

[22] UN Special Rapporteur on the Rights to Freedom of Assembly and of Association, Human rights compliant uses of digital technologies by law enforcement for the facilitation of peaceful protests, January 2024. Available at: https://www.ohchr.org/sites/default/files/2024-03/Toolkit-law-enforcement-Component-on-Digital-Technologies.pdf.

[23] See Ada Lovelace Institute. 2022. *The Ryder Review: Independent legal review of the governance of biometric data in England and Wales*. Available from https://www.adalovelaceinstitute.org/project/ryder-review-biometrics/; Fussey, P., and Webster, W. (2023) *Independent Report on Changes to the Functions of the Biometrics and Surveillance Camera Commissioner Arising from the Data Protection And Digital Information (No.2) Bill*, London: Office of the Biometrics and Surveillance Camera Commissioner. Available from https://www.gov.uk/government/publications/changes-to-the-functions-of-the-bscc-independent-report/changes-to-the-functions-of-the-bscc-independent-report-accessible.

[24] See *Glukhin v. Russia,* Judgment, ECtHR, App. No. 11519/20, 4 July 2023, para. 86.

22. This evaluation should be subject to independent expert oversight, with the authority to reject the use of a new technology, or to circumscribe its use.
23. Additional privacy-related considerations include:
    - The circumstances in which FRT is deployed. This has a significant impact on the associated harm to human rights; i.e. is FRT to be deployed across a city-wide surveillance camera network, or at a specific location for a limited time.
    - Whether FRT is used in combination with other tools. For example, is it used wholly or in part to track or to monitor; to geo-fence; or to develop pattern-of-life profiles.
    - Surveillance chilling effects are an established phenomenon and assert varied impacts depending on social location.[25] Proper assessment of surveillance-related chilling effects therefore constitute an essential consideration that must be incorporated into any harm analysis.
    - Where FRT is deployed is significant to such considerations. For example, is it deployed near a place of worship, or in a setting that holds political or cultural associations.
    - The availability of alternative measures is key to the necessity calculation. It is noted that in evaluating alternative measures the question is not can the *same task* be performed using alternative measures. It is can the *same or similar objective* be achieved. This misapplication of the necessity calculation – focusing on the tool, rather than the objective – has been a common feature of live facial recognition authorisations to date.[26]
    - The privacy impact extends beyond individuals included on the watchlist. All individuals passing through a camera's field of vision are affected.[27] It is noted that false positives affect non-watchlisted individuals.

**Question 7**

24. A general utilitarian majority view cannot be equivalenced with robust human rights respecting safeguards, consideration of minority rights, or an analysis of how such technologies affect different demographic groups in varied ways.
25. As noted, any assessment of necessity must be conducted on a use-case basis, and subject to independent expert oversight, with the authority to reject the use of a new technology, or to circumscribe its use.
26. To adequately account for the *overall* harm associated with facial recognition technology the impact on different human rights protections – such as the rights to privacy, expression, assembly, association and religion – must be assessed together in light of the interconnected, intersectional and interdependent nature of these rights. Privacy is an

[25] See, e.g., Daragh Murray, Police Use of Retrospective Facial Recognition Technology: A Step Change in Surveillance Capability Necessitating an Evolution of the Human Rights Law Framework (2023) Modern Law Review; Amy Stevens, Pete Fussey, Daragh Murray, Kuda Hove & Otto Saki, ''I started seeing shadows everywhere': The diverse chilling effects of surveillance in Zimbabwe' (2023) Big Data & Society; Daragh Murray, Pete Fussey, Kuda Hove, Wairagala Wakabi, Paul Kimumwe, Otto Saki & Amy Stevens, 'The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe' (2023) Journal of Human Rights Practice.

[26] See Fussey and Murray (2025) chapter 4 for extensive analysis of legal mandates supporting live FRT operations.

[27] *R (Bridges) v. The Chief Constable of South Wales Police* [2019] EWHC 2341, para. 62.

insufficient lens to capture the breadth of potential harms associated with this technology. Adopting a 'compound human rights harm' approach may be appropriate.[28]

27. It is important to note that privacy (and other associated rights) are connected to wider corollary implications. These include potential harms to individual identity development and democratic functioning associated with surveillance chilling effects. In light of the severity of such harms a precautionary approach should be adopted.[29]

**Question 8: Agree**

28. The necessity test requires that the seriousness of harm be assessed and evaluated. In light of the significant degree of intrusion associated with FRT, a 'high level' of justification is required.[30] This implies that any use of FRT should only be permissible in response to serious crime and that such use should be exceptional. This is a standard adopted in other jurisdictions.
29. The determination as to what constitutes serious crime should be subject to independent expert scrutiny.
30. Harm should not be evaluated in a utilitarian sense. Perceived public support cannot override human rights law protections.

**Question 9**

31. Harm should be considered in line with human rights law. A 'high level' of justification is required for *any* use of FRT. This is the baseline requirement established in case law.[31] If certain uses of FRT require more in-depth justification, this must go beyond the 'high level' required by the courts.
32. It is noted that the understanding of serious harm under the EU AI ACT (a custodial sentence of 4 years) is significantly higher than the current MPS police policy (a custodial sentence of 1 year).

**Question 10: Yes**

33. Given that the intrusive nature of FRT is well established, authorisation should be independent.[32]

**Question 11: Yes**

34. It is arguable that, given the level of intrusion, *all* uses of FRT should be subject to independent authorisation.
35. A comparable example is the establishment of the Office for Communications Data Authorisations (OCDA) to provide independent review and authorisation of communications data requests. Retention protocols also exist for other forms of biometric data (for example under the judicial functions of the Biometrics Commissioner) and

[28] See, Pete Fussey & Daragh Murray, *Facial Recognition Technology: Policing and Human Rights in the Age of Artificial Intelligence* (OUP, 2025) Section 3.3.6.

[29] See, Ronit Matar & Daragh Murray, 'Re-Thinking International Human Rights Law's Approach to Identity in Light of Surveillance and AI' (2025) Human Rights Law Review.

[30] *Glukhin v. Russia,* Judgment, ECtHR, App. No. 11519/20, 4 July 2023, para. 86.

[31] *Glukhin v. Russia,* Judgment, ECtHR, App. No. 11519/20, 4 July 2023

[32] A relevant comparator is communications data authorisations. See *Tele2 Sverige AB & Watson v. Post-och telestyrelsen & Secretary of State for the Home Department*, Grand Chamber, CJEU, Joined Cases No. C-203/15, C-98/15.

should apply to data generated by FRT to bring this technology into alignment with these other tools.

**Question 12: No, No, No**

36. Any use of FRT must be necessary in a democratic society. A key consideration here is the availability of alternative means. No evidence has been provided demonstrating the need to access other databases in the given use cases, or why existing means are inadequate.

**Question 13**

37. Not applicable. Access should not be allowed.

**Question 14: Agree**

38. The key relevant consideration is that the oversight body – or bodies – have sufficient independence, resources, expertise, and powers to operate effectively.[33]

**Question 15**

39. Any oversight body should have meaningful regulatory power to intervene, legal authority to veto operations, and be empowered to investigate compliance with legal standards

**Question 16**

40. A regulator should be distinguished from a standard setting body.
41. Any regulator should be able to access independent expertise.
42. FRT is a socio-technical system. Evaluation therefore requires inter-disciplinary expertise and is not reducible solely to a matter of algorithmic testing. This includes assessment of the value and quality of human decision-making implicated in FRT use.
43. Any regulator, and any independent experts called upon, must be able to scrutinise the evidence used to justify deployments, and the operation of FRT in practice

**Question 17**

44. A regulator should be distinguished from a standard setting body.
45. The considerations raised over the course of this consultation, are complex issues implicating technology, society and the law. Any regulator should be able to access appropriate independent expertise.
46. Any evidence should meet scientific standards of peer review. Any evaluation of that evidence should adhere to standards of ecological validity, and therefore closely approximate real life uses (including the role of human decision-making).
47. FRT is a socio-technical system. Evaluation therefore requires inter-disciplinary expertise and is not merely a matter of algorithmic testing. This includes assessment of the value and quality of human decision-making implicated in FRT use.
48. Any regulator, and any independent experts called upon, must be able to scrutinise the evidence used to justify deployments, and the operation of FRT in practice.

[33] See, e.g. Daragh Murray, Pete Fussey, Lorna McGregor & Maurice Sunkin, 'Effective oversight of large-scale surveillance activities: A human rights perspective' (2021) Journal of National Security Law and Policy.