INDEPENDENT REVIEWER OF TERRORISM AND STATE THREAT LEGISLATION

RESPONSE TO BIOMETRICS CONSULTATION 2025/6

1. This document responds to the government's consultation entitled "New legal framework for law enforcement use of biometrics, facial recognition and similar technologies" (4.12.25).

2. I agree that the current legal framework neither gives the police sufficient confidence to use technologies such as facial recognition where appropriate, nor provides the public with confidence that such technologies are being used responsibly according to sufficiently clear and accessible standards.

3. I also echo the observations of the Centre for Emerging Technology and Security (part of the Alan Turning Institute) that disagreements over fundamental biometric technologies have undermined the ability to revise existing regulatory frameworks[1].

4. This response principally concerns the question of whether a new framework, and the work of a new single regulator, should cover not just existing but emerging technologies that could be highly relevant to police work in protecting national security:

    - Examples of emerging biometric technologies given in the consultation document are voice and iris recognition.
    - The government also has in mind so-called 'inferential' technologies which analyse the body and its movements to infer information about the person, such as their emotions or actions.
    - Examples given in the consultation are polygraphing or analysing CCTV to identify collapsed or injured people or potential suicides pacing a well-known hotspot.

5. In my report *Terrorism Acts in 2023* (published July 2025), I referred to emerging technologies that have been supercharged with Artificial Intelligence, with machines capable of picking out revealing patterns in the form of vein analysis, gait analysis, handwriting analysis, keystroke analysis, behavioural analysis,

[1] Stockwell, S., Hughes, M., Ashurst, C., Ni Loideain, N., 'The Future of Biometric Technology for Policing and Law Enforcement: Informing UK Regulation' (2024).

linguistic analysis and emotional analysis[2]. The power of technology, and the availability of data (for example, aggregated doorbell footage, or cloud data accessible from personal devices), is increasing.

6. In my report I also suggested that machines will inevitably be trained from single or multiple types of data to develop further deep insights, such as insights about a person's ethnicity or health (including pregnancy), sexuality, marriage status or political leanings.

7. This raises the privacy stakes if such insights are used by law enforcement[3]. It is highly plausible that many if not all of these intimate insights are already being generated by the major tech companies for the purpose of advertising.

8. Some conceptual brush-clearing is required:

    - It may be that some inferential insights could (now or in the future) allow or confirm unique identification. This would put them in the same category as fingerprints or DNA[4].
    - On the other hand, it could be argued that there is something about fingerprints or DNA (for example, that they are immutable aspects of our bodies) that distinguishes them from other identifying features such as behavioural tics.
    - Other inferential insights might say a great deal about an individual but not allow that person to be uniquely distinguished from others.
    - As to the latter, although it is scary to consider what Artificial Intelligence may be able to infer, in principle this may not be different from old-fashioned detective work – e.g. drawing inferences from evidence or compiling a profile to help identify a potential terrorist, perhaps guided by insights from behavioural science – albeit souped up by computer power.

9. Sound categorization is relevant to any changes to the system of National Security Determinations (NSD) which currently regulate the retention of fingerprints and DNA for national security purposes, under the supervision of Biometrics Commissioner[5]. It may be that in future, depending on the above analysis, and any

[2] At paras 4.32-4.48.
[3] As long ago as 2018, the Technical Advisory Panel to the Investigatory Powers Commissioner noted the capability of AI to increase privacy considerations, because it could be used to generate highly personal insights from apparently bland data: Report of Metrics of Privacy Conference (14.11.18).
[4] See the definition of 'biometric data' in section 205(1) Data Protection Act 2018.
[5] Established by the Protection of Freedoms Act 2012.

genuine practical considerations, other forms of biometrics should be added to the NSD scheme.

10. Sound categorization is also relevant to how these types of emerging technologies should be regulated under one legislative scheme or subject to a single regulator.

11. There is a risk of unintended consequences – for example, stifling police use of current or future techniques that many of us take for granted in our own work (such as the use of AI), or encouraging officers to use computers away from the office.

12. In addition, I suggest that *privacy considerations* are not the only important factor when judging the acceptability of identifying technologies. Sometimes it is the mere possibility that the authorities are spying on you that makes ordinary life less comfortable: for example, whether or not it is working, or making a permanent record, the presence of yet another CCTV camera in a social or civic space can create the uncomfortable feeling of being watched or suspected. That feeling may be a necessary aspect of security but should not be taken for granted. I therefore doubt that the Information Commissioner is an ideal single regulator given their remit under the Data Protection Act 2018.

13. Conversely, I remain concerned that insufficient attention is given to the internet as a key source of data from which emerging technologies are likely to draw their inferences. The consultation refers to the question of whether data is acquired and/or used "in a public or a private space, and the nature of the public or private space" but it is unclear whether this is intended to refer to online spaces, or how to distinguish between what is public online and what is private online[6].

14. There is no express reference in the consultation to the huge amounts of personal data online, much of it posted openly and/or surrendered to tech companies for advertising purposes, or the question of whether and if so to what extent analysing this data interferes with a person's privacy.

    - A serious effort to address this question *has* been made in recent iterations of the Covert surveillance and property interference Code of Practice issued under the Regulation of Investigatory Powers Act 2000[7].
    - I do not see how the questions in the consultation can be answered (a) without greater attention to the implications of online data and (b) without

[6] This is notoriously difficult. With Professor Stuart Macdonald I have written about this in a briefing note, 'Online Safety Bill: Distinguish between public and private communication' (1.3.23).
[7] The most recent version of the Code is dated 22.2.24.

considering the impact of the current framework for regulating investigatory powers.

- For completeness, I fear that the existing Code too readily encourages police to seek an authorisation for directed surveillance when analysing readily available online information.

15. It follows from these difficult but as yet unanswered questions, that:

- Firstly, I would urge caution about inviting Parliament to pass a detailed single legislative framework against which to judge the lawfulness of police use of emerging technologies.
- Secondly, any independent regulatory or supervisory body, which I agree must be independent, should have made available to it considerable technical and academic expertise (akin to the Investigatory Powers Commissioner's Technical Advisory Panel) so that it can consider these difficult questions in the light of emerging practice.
- Thirdly, consideration should be given to enabling the independent regulator or supervisory body to issue provisional permissions for the use of novel technologies, according to principled criteria. These provisional permissions could be revisited, evaluated, and extended or not. This would allow law enforcement authorities, such as Counter Terrorism Police, to use emerging technologies in a controlled and supervised way without having to wait for new legislation.

JONATHAN HALL KC

22 JANUARY 2026