Joint statement on facial recognition technology

The government has announced in the King's Speech that the Police Reform Bill will include a framework for police use of facial recognition. If a new framework is to establish conditions for the lawful use of FRT, the recommendations below **collectively** represent the **minimum, necessary protections** for use that will meaningfully protect our individual and collective privacy, free expression and free association rights and the democratic freedoms that flow from it.

While many signatories believe facial recognition represents unacceptable risks to our human rights in many contexts, the recommendations are pragmatic in delimiting its use to strictly necessary and proportionate cases, comparable to the limitations under European law. The safeguards interlock and work together; they would provide less than the sum of their parts if cherrypicked. They are scoped to the announcements in the King's Speech; if legislation proposes broader circumstances for FRT deployment, more robust safeguards will inevitably be required. Because they are constitutional safeguards, they must be be baked into the legislation itself, not deferred into easily-amendable codes of practice or guidance. They represent the minimum standard the Bill must meet in order to provide a clear, coherent and sustainable framework for facial recognition that mirrors our democratic counterparts, whilst offering some protection to the general public from excessive AI surveillance.

Big Brother Watch
Ada Lovelace
Article 19
End Violence Against Women Coalition
Glitch
JUSTICE
Liberty
Open Rights Group
Race Equality First
Rights of Women
Statewatch

Live Facial Recognition

1. All uses of LFR should be prohibited except in the strictly defined circumstances set out below.
2. Only law enforcement bodies should be able to deploy LFR and only for strictly defined policing purposes.
    - The definition of law enforcement bodies includes all police forces in England and Wales and specialist law enforcement agencies like the British Transport Police and National Crime Agency. It excludes other non-law enforcement bodies that conduct law enforcement activity.
3. LFR may only be used in the following strictly defined policing purposes:

a) 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;

b) The localisation of an adult for whom there are reasonable grounds to believe they have committed a serious criminal offence.

Serious criminal offence is to be defined as:

- Qualifying offence under s65A of the PACE 1984; and
- where the sought person could reasonably be expected to be sentenced to imprisonment for a term of no less than four years.

c) The targeted search for specific victims of kidnapping, trafficking in human beings or sexual exploitation of human beings, as well as the search for high-risk missing persons.

4. Any images of a sought person to be included on a watchlist must:

a) be obtained and held lawfully by the law enforcement body

b) be the most up to date and/or suitable image that is of appropriate quality (having regard to the source, age, clarity and quality of the image)

c) not be composite images (such as an e-fit, police sketch, photofit, DNA phenotyping)

5. There must be a nexus between the geographic scope of the deployment and the persons sought for each LFR deployment. Any officer proposing to place an individual on a LFR watchlist must have reasonable grounds to believe that each individual sought person on the watchlist will be present at the proposed deployment location.

6. Where LFR is deployed for purposes 3(b) or (c), law enforcement agencies must exhaust targeted, more proportionate means of locating each sought person on a case-by-case basis before placing them on a LFR watchlist. These attempts must be documented for subsequent review. This may include, but is not limited to, house-to-house enquiries, obtaining CCTV footage, searching the area where the sought person was last seen, public appeals for information, intelligence gathering.

7. Where LFR is used for the purposes of use case 3(b) and 3(c), it must not be deployed in locations engaging greater expectations of privacy, where special category data is likely to be processed, or where additional rights and freedoms are engaged in addition to privacy, including freedom of expression, freedom of assembly and association, and freedom to manifest one's religion or beliefs. This

includes, but is not limited to, schools, places of worship, health centres, polling stations, protests and lawful assemblies.

8. Live facial recognition may only be deployed when a (officer of Superintendent ranking) deems it necessary and proportionate to do so. The rationale for the necessity and the proportionality of the deployment, and the quality of the intelligence justifying it, must be recorded in a human rights impact assessment completed by the deploying law enforcement body and provided to the authorising body.
9. Each LFR deployment should require prior authorisation by a judicial authority or an independent administrative authority whose decision is binding. In circumstances of genuine urgency, the law enforcement body can obtain post-deployment authorisation within 24 hours. The authorising body must only authorise LFR deployments which are necessary and proportionate to the human rights interference involved, having regard to:
    a) the obligatory human rights impact assessment;
    b) the quality of the intelligence justifying the deployment;
    c) the geographical relevance of the deployment location;
    d) the extent to which less intrusive methods have been exhausted; and
    e) the impact of the deployment on specifically vulnerable groups, including children.
10. Each deploying law enforcement body must monitor and publish the outcomes of LFR deployments quarterly, including number of faces scanned, outcomes of matches (i.e., arrest, no further action, conviction, false match), demographic data, and the geographical proportion of public space subject to LFR deployment(s) in that quarter, relative to the total area of any territorial law enforcement body's responsibility.

Retrospective Facial Recognition

11. RFR may only be used by law enforcement bodies for investigation of adults suspected of serious crimes as defined by s65A of the PACE 1984, where the sought person could reasonably be expected to be sentenced to imprisonment for a term of no less than four years. It must not be used for the investigation of victims, witnesses or associates.

    a) The definition of law enforcement bodies includes all police forces in England and Wales and specialist law enforcement agencies like the British Transport Police and National Crime Agency. It excludes other non-law enforcement bodies that conduct law enforcement activity.

12. Probe images of a sought person to be included on a watchlist must:

    a) be held and obtained lawfully by the law enforcement body

    b) be the most up to data and/or suitable image that is of appropriate quality (having regard to the source, age, clarity and quality of the image)

    c) not be a composite image (such as an e-fit, police sketch, photofit, DNA phenotyping)

13. Law enforcement bodies are only permitted to use lawfully-held custody images as image reference databases for RFR searches. It must be prohibited to use the following as an image reference database in any future circumstance:

    a) databases that have been created or expanded through the untargeted scraping of facial images from the internet or CCTV footage;

    b) databases comprising of non-police originated images; and

    c) databases that comprise of a significant portion of the population and do not process images for the primary purpose of the investigation, prosecution and/or conviction of any criminal offence (i.e., passport, DVLA, digital ID databases).

14. A RFR match should not automatically make someone a suspect or be treated as a confirmed identification absent additional checks.

15. Before using RFR, law enforcement agencies must exhaust less intrusive means of identifying each sought person on a case-by-case basis. These attempts must be documented for subsequent review. This may include, but is not limited to, house-to-house inquiries, obtaining CCTV footage, searching the area where the sought person was last seen, public appeals for information, intelligence gathering.

16. Law enforcement bodies must be required to keep detailed records of their reasons for deploying RFR on a case-by-case basis, which should be open to subsequent scrutiny by the oversight body.
17. Each deploying law enforcement body must monitor and publish the outcomes of RFR deployments quarterly, including number of uses, the tools and thresholds used, outcomes of matches (arrest, no further action, charge, caution, conviction, wrong ID) and demographic data.

Oversight Body

18. The Oversight Body must have, inter alia, the powers to:

    a) conduct post facto reviews of both individual uses of LFR and the systemic approach to FRT taken by law enforcement. Such reviews should include whether necessity and proportionality assessments have been accurately and consistently balanced; the impact on human rights including privacy and freedom of assembly and association; and equality and discrimination impacts.

    b) Require algorithms used to be scientific valid for accuracy and reliability (including demographic non-discrimination), and set validation testing requirements;

    c) Set standards for design, including data quality, deployment, including thresholds used, and performance, including accuracy and equitability.

    d) Have the power to audit, inspect, require information, demand compliance with standards, and where standards are not complied with, apply for an injunction to prohibit the use of a tool;

    e) Responsibility to publish an annual report before Parliament.