February 2026

Privacy International's Submission to the UK Home Office Consultation on a Legal framework for law enforcement use of use of biometrics, facial recognition and similar technologies

About PI

Privacy International ("PI") is a registered charity (no 1147471), that works globally at the intersection of modern technologies and rights.[1] Established in 1990, PI undertakes research, litigation and advocacy to build a better future where technologies, laws and policies contain modern safeguards to protect people and their data from exploitation.

PI has long documented the impact of biometric technologies including facial recognition technologies (FRT) on people and their rights.[2] In particular, our campaign 'The End of Privacy in Public'[3] has been monitoring the continued roll out of FRT throughout the UK in the absence of a legal framework and the subsequent risks this has for the enjoyment of human rights.

Introduction and background

PI welcomes the government's consultation to develop a new legal framework for the use of biometric technologies including FRT by law enforcement.

This is an important development considering the rapid deployment of biometric technologies across the United Kingdom. London's Metropolitan Police Service (the Met) have reportedly scanned around 1 million faces between January and May 2025[4] and 4.7 million faces in 2023.[5] There are now also permanent live FRT cameras in Croydon, South London,[6] and in use at major

[1] See: https://privacyinternational.org/
[2] Privacy International, Facial Recognition, https://privacyinternational.org/learn/facial-recognition
[3] See: https://privacyinternational.org/campaigns/end-privacy-public
[4] Catherine Levin, 10 things to know about Live Facial Recognition technology, *Emergency Service Times*, 2 May 2025, https://emergencyservicestimes.com/2025/05/02/10-things-to-know-about-live-facial-recognition-technology/
[5] Nadeem Badshah, Met police to more than double use of live facial recognition, *The Guardian,* 31 July 2025, https://www.theguardian.com/technology/2025/jul/31/met-police-to-more-than-double-use-of-live-facial-recognition
[6] Sonja Jessop, Facial recognition pilot cuts crime, says Met, *BBC News*, 19 January 2026,

transport hubs[7] and for immigration enforcement.[8] London is turning into one of the most heavily surveilled capitals in the world.

In relation to questions 6 & 7 of the consultation, these technologies pose a major risk to human rights under the European Convention of Human Rights (ECHR) brought into domestic application by the Human Rights Act 1998. Their often-indiscriminate use amounts to mass surveillance, which is usually deployed without consent, which may undermine the rights to privacy and data protection (Article 8, ECHR). The infringement on the right to privacy poses a further risk to the exercise and enjoyment of concomitant rights. If people are aware they are being surveilled, they may alter their behaviour, dissociate with certain groups or avoid attending a protest – undermining their rights to freedom of expression, assembly and association (Articles 10 & 11, ECHR). Use of this technology has also been found to be discriminatory (Article 14, ECHR) – a recent report revealed bias in police facial recognition technology because it's "more likely to flag black and Asian people than their white counterparts."[9] This reinforces historical injustices and existing inequalities.

Considering question 6 of the consultation, an interference with the right to a private and family life under Article 8 of the ECHR cannot be lawful unless it satisfies the requirements of Article 8(2) of the ECHR. Specifically, the interference must be in pursuit of a legitimate aim, be in accordance with the law, and necessary in a democratic society. To be in accordance with the law, it must have a basis in domestic law and be compatible with the rule of law. Compatibility with the rule of law requires compliance with the requirements of accessibility and foreseeability, and it must contain sufficient constraints against arbitrary or disproportionate use.[10]

Despite the risk they pose, and these human rights requirements, biometric technologies, particularly FRT, have been deployed without adequate oversight or safeguards. The existing patchwork of laws does not meet these requirements. The development of the legal framework at issue in this consultation accordingly represents an important moment to get this right. Considering this, we wish to highlight three things:

- First, the starting point should always be to examine whether these technologies should be deployed at all, or whether less intrusive means can be used. Relatedly, certain technologies that pose too grave a harm should be prohibited.

---

https://www.bbc.co.uk/news/articles/c2056r07rjlo

[7] Masha Borak, British Transport Police to trial live facial recognition on railway stations, *Biometric Update*, 27 May 2025, https://www.biometricupdate.com/202511/british-transport-police-to-trial-live-facial-recognition-on-railway-stations

[8] See: https://www.gov.uk/government/collections/live-facial-recognition-in-immigration-enforcement

[9] Rachel Hall, Urgent clarity' sought over racial bias in UK police facial recognition technology, *The Guardian,* 5 December 2025, https://www.theguardian.com/technology/2025/dec/05/urgent-clarity-sought-over-racial-bias-in-uk-police-facial-recognition-technology

[10] *R (Bridges) v Chief Constable of South Wales Police* [2020] 1 WLR 5037 (CA),[80]

- Second, the scope of this framework is unclear. It appears to broadly apply to biometric technologies, and specifies certain ones including: FRT, inferential, operator-initiated technologies, and object recognition technologies. However, it fails to mention gait analysis and iris recognition. In some instances, the framework poses questions relating to specific technologies, and in others, refers to all biometric technologies more broadly. We appreciate the consultation acknowledges this confusion and questions the scope of the framework. However, important consideration should be given to the scope of its application. The level of intrusiveness of biometric technologies and related infringement on rights varies according to the type of technology and how it is used. Because of this, the legal framework should explicitly specify which technologies it applies to. It should specify the legal basis and conditions for use, and the relevant unique safeguards that apply to each technology. Considering question 4 of the consultation we recommend that the legal framework should be technologically specific – it should explicitly state the technologies it applies to. If new or emerging technologies are to be included in its scope, the primary law should be amended.

- Third, we are concerned that whilst the Home Office has been publicly consulting on this legal framework, they have concurrently announced that "the number of live facial recognition vans will increase five-fold, with 50 vans available to every police force in England and Wales to catch violent and sexual offenders."[11] This announcement undermines the consultation process, and raises concerns that the resulting legal framework would serve merely as a rubber stamp to continue to deploy biometric technologies in a way that infringes upon human rights, paving the way for a surveillance state.

Considering the need for the framework to be technologically specific, our submission engages primarily with FRT – live, retrospective and operator initiated. Where we are able to comment on additional technologies we do so.

Summary of the necessary safeguards (In response to questions 1-4 & 6-10)

For the deployment of FRT to comply with human rights law and standards it should be subject to the overarching principles of necessity, proportionality and legality. The legal framework should outline restrictions, safeguards and conditions of its use to comply with these principles to prevent abuse. Below is a list of essential safeguards for FRT which should be included in the legal framework, some of which are expanded on in other sections:

1. **Prescribed by law:** FRT should not be used unless authorised and regulated by law. The law should be accessible, and provide the public with an adequate indication of the circumstances and conditions under which authorities can deploy and use FRT. Specifically, the law should provide details about:

[11] Home Office, 'News story: White paper sets out reforms to policing', 26 January 2026, https://www.gov.uk/government/news/white-paper-sets-out-reforms-to-policing

1.1. Prohibited and lawful uses. Specifically, the following uses should be prohibited:
   1.1.1. Live facial recognition technology (LFRT);
   1.1.2. Operator initiated technology (OIFRT);
   1.1.3. Inferential technology;
   1.1.4. To Identify whistleblowers, journalists or journalistic sources;
   1.1.5. To categorise people by a protected characteristics;
   1.1.6. To Identify protesters or to collect information on people attending peaceful assemblies and;
   1.1.7. To Identify people in or around polling stations.[12]
1.2. The scope of the law, specifically which technologies it applies to. The primary legal framework should be appropriately amended if new and emerging technologies should be included in its scope.
1.3. The temporal considerations which categorise FRT use as either retrospective or live.
1.4. The safeguards that guard against arbitrary and disproportionate use (listed below).[13]
1.5. The specifications for probe images for FRT: Safeguards should be put in place that ensure a quality standard for probe images and guard against tampering. Such standards should consider the source of the image, its age, the quality of the image, whether there is anything obstructing the image, the chain of custody of the image, and whether any rights have been violated in obtaining the image.
1.6. Details about the requirements to use a database including how to assess whether its use is necessary and proportionate, the circumstances under which they may be accessed, and the safeguards in place to limit the interference with the rights of the people in the databases.
1.7. Provisions regarding requirements for training and impact assessments.

2. **Legal basis of use:** The use of FRT should be necessary, and proportionate. This means firstly, that deploying this kind of technology would be the least intrusive means of achieving similar identification results, compared to other available policing techniques. Secondly, that the use of biometric technologies should be limited to the following, clearly defined purposes:
   2.1. 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.
   2.2. 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.
   2.3. The identification of suspects or perpetrators of exhaustively listed serious crimes.[14]

3. **Prior Judicial authorisation:** Law enforcement should not be permitted to deploy FRT, unless there is prior judicial authorisation for such use, except in duly justified urgent

[12] INCLO, Eyes on the Watchers: Challenging the Rise of Police Facial Recognition, 2025, https://inclo.net/wp-content/uploads/2024/03/INCLO-FRT-Principles-Final.pdf;
[13] *R (Bridges) v Chief Constable of South Wales Police* [2020] 1 WLR 5037 (CA),[80].
[14] Article 5, EU AI Act, https://artificialintelligenceact.eu/article/5/

cases[15], whereby a higher-ranking officer, wholly independent of the investigation, must give prior approval.[16] In such exceptional cases, the judicial authorisation must still be requested without undue delay and no later than 48 hours after the use.[17]

4. **Reference databases:** The use of private databases should be prohibited. The use of any government database should be authorised by law, and its use should receive prior judicial authorisation when requested at the time of deployment. Databases may only be accessed if doing so is necessary and proportionate. The law should provide sufficient detail to the public about which databases may be used, and the circumstances and conditions under which they may be accessed. Specifically, the law should require and include details concerning:
    - 4.1. An assessment of whether use of the database for the stated biometric surveillance purpose is necessary and proportionate.
    - 4.2. The criteria used to assess whether a database is fit for purpose and may be used for biometric searches. This should include an assessment of the technical specs of the database including whether there are any data protection, discrimination or other human rights concerns.
    - 4.3. The procedure for prior judicial authorisation for the use of a database for a particular search;
    - 4.4. Details about how the database is accessed (e.g whether law enforcement is given direct access to a database or whether a search is run by the database owner on behalf of law enforcement);
    - 4.5. The safeguards in place to mitigate against any identified harms;
    - 4.6. Usage;
    - 4.7. Storage;
    - 4.8. Retention;
    - 4.9. Access of third parties;
    - 4.10. Procedures for preserving the integrity and confidentiality of data;
    - 4.11. Procedures for destruction;
    - 4.12. Oversight mechanisms, including the requirement to keep a record of the requests to access a database. The record should note whether the requests were accepted or rejected, and the reasons why.

5. **Transparency:** the law should require the publication of certain information, including:
    - 5.1. The number of deployments, including details about where and when it was deployed.
    - 5.2. The number of FRT searches run by each law enforcement body;

---

[15] Under the Investigatory Powers Act 2016 urgent circumstances refer to situations where an immediate need for surveillance—such as an imminent threat to life, serious harm, or a fast-moving investigative opportunity—makes it impossible to wait for the standard, two-stage approval process (known as the "double lock"). In these cases, the law provides for a fast-track process, allowing warrants to be issued without prior Judicial Commissioner approval, although they must still be approved shortly afterwards.

[16] INCLO, Eyes on the Watchers: Challenging the Rise of Police Facial Recognition, 2025, https://inclo.net/wp-content/uploads/2024/03/INCLO-FRT-Principles-Final.pdf

[17] Under the EU AI Act prior authorisation or without undue delay is to take place within 48 hours and if rejected the FRT must be stopped and any data collected will be deleted.

5.3. The number of times a particular reference database is searched for the purposes of FRT by each law enforcement body;
5.4. The number of searches that generated leads;
5.5. The number of searches that lead to an arrest or charge;
5.6. The number of misidentifications;
5.7. The demographic breakdown of the probe images used, specifying gender, race and any other relevant protected characteristics;
5.8. Aggregated, de-identifiable information concerning the number of requests made for authorisation, including the lawful basis relied on, the outcome of the request and the databases authorised for use; and
5.9. Annual reports by the oversight body which include the number of complaints received, errors uncovered, and the outcomes.

6. **Independent oversight body:** An independent body should be established to ensure FRT, and other biometric technologies are deployed in compliance with the law. It's establishment, powers, role and obligations should be regulated by law. The law should specify the scope of oversight noting the technologies and bodies it oversees. In order to function effectively the body should be structurally and functionally independent, sufficiently resourced and staffed with a range of subject matter and technological experts. The body should be empowered and equipped to hear and respond to complaints from members of the public and to conduct its own investigations. This requires the body to be authorised to access the necessary information, compel disclosure and impose remedies and penalties. The oversight body should be required to report to the public and Parliament annually.

7. **Disclosure to people detained, arrested and charged:** To enable the right to fair trial[18], any person detained, arrested and charged as a result of, or related to, the use of FRT by law enforcement should be provided with the following information:
   7.1. Details about the technology used, including information concerning the manufacturer of the technology, its source code and the data that was used to train it;
   7.2. The reason and process for authorisation of deployment;
   7.3. Details about the date, time and ways in which the technology was deployed;
   7.4. Details concerning the authorisation and use of certain reference databases;
   7.5. Details about the probe image including its source and quality, and access to the probe image should be provided;
   7.6. Details about the probability score or findings made by the FRT system; and
   7.7. Details regarding the role of private companies in the preparation of surveillance information for use as evidence including all processing operations relating to raw data.[19]

Expansion on certain safeguards (In response to questions 1-4 & 6-10)

[18] Article 6, ECHR, https://www.echr.coe.int/documents/d/echr/convention_ENG
[19] Privacy International, Protest Surveillance into Courts, https://privacyinternational.org/sites/default/files/2025-01/Protest-surveillance-into-courts.pdf

We expand on some of the above aspects of the legal framework below.

1.1 Prohibited Uses

1.1.1 Live FRT (LFRT)

PI recommends that the legal framework should prohibit the use of LFRT by law enforcement in public spaces. Given the intrusive nature of LFRT, coupled with its mass, indiscriminate use, we submit that it's deployment can never meet the requirements of proportionality. Proportionality requires that the least restrictive measure is used to achieve a legitimate aim.[20]

LFRT is highly intrusive because it relies on the capture, extraction, storage or sharing of people's biometric facial data – which is as unique to individuals as their fingerprint - often without their explicit consent.[21] The deployment of LFRT is indiscriminate – it subjects everyone within a public space, including those not suspected of wrongdoing, to surveillance.

LFRT is being deployed in public spaces with heavy footfall for example, on public transport[22], major transport stations[23], and international sports events.[24] For example, it has been reported that The Met's deployment of LFRT at London Underground stations can process the biometric data of up to 50 000 people a day.[25] Over three million people have been scanned with police facial recognition cameras in the past year in London alone.[26] A single deployment can accordingly infringe on the rights of thousands, if not millions of people.

The harm of such an intrusion far outweighs its usefulness. It has been reported that more than 400,000 faces have been scanned by police in the south of England using LFRT but the scans only lead to a handful of arrests, some of which were for shoplifting, a minor offence.[27] The Met's 2025 annual report on LFRT shows that across the reporting year there were 962 arrests, 549 people (57%) were arrested because there was a warrant for their arrest issued by the courts, and 347 (36%) were in cases where the person was wanted by the Met because there were

---

[20] Kasmiri v Secretary of State for the Home Department [2007] UKHL 11
[21] Privacy International, UK MPs asleep at the wheel facial recognition technology spells the end of privacy in public, http://privacyinternational.org/long-read/5155/uk-mps-asleep-wheel-facial-recognition-technology-spells-end-privacy-public
[22] Ross Lydall, Tube fare dodging: live facial recognition cameras could be used to catch most prolific evaders, *The Standard*, 9 July 2025, https://www.standard.co.uk/news/transport/facial-recognition-cameras-fare-dodging-tube-london-underground-tfl-b1237049.html
[23] Holly Brencher, London Bridge station is part of six-month live facial trial, *London Now*, 11 February 2026, https://www.london-now.co.uk/news/25846169.london-bridge-station-part-six-month-live-facial-trial/
[24] Vas Panagiotopoulos, Soccer Fans, You're Being Watched, *Wired*, 3 November 2022, https://www.wired.com/story/soccer-world-cup-biometric-surveillance
[25] Bill Curtis and Charles Hymas, Met recognition cameras catch 50,000 faces a day, *The Telegraph,* 24 September 2025, https://www.telegraph.co.uk/news/2025/09/24/met-police-recognition-cameras-catch-50000-faces-day-london/
[26] Jess Warren, No arrests from false facial recognition alerts, *BBC News,* 31 October 2025, https://www.bbc.co.uk/news/articles/c4gp7j55zxvo
[27] Nathan Briant, Police using facial recognition: Is it a problem?, *BBC News*, 21 January 2026, https://www.bbc.co.uk/news/articles/cddg5y36j88o

reasonable grounds to suspect that the individual is about to commit, is committing or has committed a recordable offence.[28] Of those 347 arrests a significant number of them were for lower level offences such as theft and criminal damage.[29] This is a small number of arrests compared to the privacy invasion for the 3, 147, 436 faces that passed through the camera zones.[30] The fact that these people had their highly sensitive facial data processed unknowingly to conduct these arrests strongly undermines police claims of FRT being a "targeted" measure.

There are already serious concerns with how UK police forces compile watch lists for LFRT deployments, arguably in a disproportionate and discriminatory way that raises a range of human rights concerns. It has been reported that comparing data from 2020 to 2022, the number of people on FRT watch lists has gone from about 6,500 to more than 16,000 in 2025.[31] The police's compilation of watch lists was also raised by the Court of Appeal in *R (Bridges) v Chief Constable of South Wales Police*, which found that the police had too broad a discretion when deciding who should be on the watch lists used for FRT.[32]

Furthermore, Liberty Investigates found that hundreds of children have been included in watchlists by police forces across the UK, including children as young as 12 for the purpose of FRT. They also found that police forces had interpreted current guidance on including children on watchlists differently – while forces did not keep records to explain why children had been included in the first place.[33]

Currently the College of Policing provides guidance to police forces on how they compile a watchlist for LFRT purposes.[34] The guidance states that the watch lists can include victims and witnesses, as well as photographs obtained via non-police sources. This gives police forces unclear boundaries and enables individual police forces to decide at their own discretion who can be on a watchlist for a LFRT deployment. For example, Sussex and Surrey Police reportedly have people on their FRT watch lists who are subject to court orders, wanted on recall to prison or suspects in criminal investigations, which is quite a wide range of reasons for inclusion,[35] again raising concerns with proportionality.

---

[28] The 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

[29] Ibid.

[30] The 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 page 15.

[31] Ayang Macdonald, UK privacy concerns mount as police facial recognition scans surpass 50k a day, *Biometric Update*, 25 September 2025, https://www.biometricupdate.com/202509/uk-privacy-concerns-mount-as-police-facial-recognition-scans-surpass-50k-a-day#:~:text=Live%20feeds%20from%20faces%20scanned%20by%20the,to%20identify%20those%20on%20the%20police%20watchlist.

[32] *R (Bridges) v Chief Constable of South Wales Police* [2020] 1 WLR 5037 (CA),[80].

[33] Liberty, Children on facial recognition watchlists shows need for safeguards, 1 December 2025, https://www.libertyhumanrights.org.uk/issue/liberty-children-on-facial-recognition-watchlists-shows-need-for-safeguards/

[34] College of Policing, Authorised Professional Practice: Live Facial Recognition, https://www.college.police.uk/app/live-facial-recognition/watchlist

[35] Jadzia Samuel, Jack Fiehn and Patrick Barlow, Facial recognition vans 'not about surveillance, *BBC News*, 13 November 2025, https://www.bbc.co.uk/news/articles/clykr14glnwo

At the international level, the UN Special Rapporteur on the right to privacy has voiced explicit concerns over the use of FRT in public spaces stating that: "recording, analysing and retaining facial images of individuals without their consent constitute interference with their right to privacy. By deploying facial recognition technology in public spaces, which requires the collection and processing of facial images of all persons captured on camera, such interference is occurring on a mass and indiscriminate scale".[36]

Furthermore, the United Nations High Commissioner for Human Rights, has called on states to "impose moratoriums on the use of potentially high-risk technology, such as remote real-time facial recognition, until it is ensured that their use cannot violate human rights", pointing towards people being wrongly "arrested because of flawed facial recognition".[37] The High Commissioner went on to call for greater transparency and express fears that the long-term storage of data obtained by such technology "could in the future be exploited in as yet unknown ways".[38]

The European Union Artificial Intelligence Act (EU AI Act),[39] provides an example of how to regulate artificial intelligence including LFRT, based on the level of risk they pose. Under the EU AI Act LFRT is prohibited for law enforcement purposes, unless it is strictly necessary.

Overall, we believe the use of LFRT is a disproportionate interference with privacy. It is a mass surveillance tool creating a chilling effect, with consequences for democracy and concomitant human rights. Therefore, LFRT should be prohibited in the new legal framework, and its use immediately halted.

1.1.2 Operated Initiated FRT (OIFRT)

The consultation document provides that OIFRT is a relatively new capability and is only being used by two police forces. It is a mobile app which allows officers on the street to conduct an identity check against the custody image database, without having to take the person being checked into custody.[40] Whereas South Wales Police describe the use of OIFRT as comparing a photograph of a person's face taken on an officer's mobile phone to the predetermined watchlist to identify a subject.[41] From the outset there appears to be conflicting public information around whether the captured image is compared to the Police National Database

[36] Report of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, 13 September 2021, A/HRC/48/31, https://www.ohchr.org/en/calls-for-input/2021/right-privacy-digital-age-report-2021
[37] Office of the High Commissioner for Human Rights, Press Release: Artificial intelligence risks to privacy demand urgent action – Bachelet, 15 September 2021, www.ohchr.org/en/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet
[38] Ibid.
[39] EU AI Act, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689
[40] Home Office, New legal framework for law enforcement use of biometrics, facial recognition and similar technologies. Government consultation, Pg 7, December 2025, https://assets.publishing.service.gov.uk/media/69318bb2cdec734f4dff4257/PDF_Consultation_FINAL.pdf
[41] See: https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/?dongs

which contains custody images or a predetermined watchlist which could include images from other sources.

We believe OIFRT should not be permissible under the new legal framework as it poses too high a risk to human rights. Its ability to be used to process individual's highly sensitive biometric data to identify individuals on the spot is highly concerning. We believe that providing police officers directly with this technology would likely lead to 'function or mission creep'[42] with the potential to be used in an authoritarian and discriminatory way. There is a likelihood that this tech would be disproportionately used against marginalised communities including migrants, and those who look like migrants. This derives from existing concerns with stop and search data which consistently shows that Black and Asian minority ethnic groups are disproportionately targeted,[43] which could be replicated with the use of OIFRT.

Furthermore, considering required safeguards and conditions upon which FRT may be used (discussed in further detail below under 'safeguards'), we do not believe that OIFRT could meet these conditions. For example, the need to gain prior judicial authorisation.

1.1.3 Inferential Technologies

Inferential recognition technologies refer to emotion or behaviour recognition technologies for the purpose of detecting and predicting human conditions or intentions, such as anger, fear, or predicting a crime.[44] The consultation document gives examples for uses of this tech including detecting whether someone has collapsed or is injured, pacing in a suicide hotspot or being untruthful in a polygraph.

By design, emotion recognition technologies are fundamentally flawed, with poor accuracy and scientific grounding, and use discriminatory methods.[45] They remain contested and even referred to as "pseudoscientific".[46]

Other research shows that monitoring physical and behavioural attributes, for example, measuring eye-tracking, can be linked to further categorisation and profiling as they can reveal other attributes such as age, gender, ethnicity, sexual preference and medical diagnoses such as attention deficit hyperactivity disorder (ADHD) and autism.[47] Therefore, they raise concerns around the right to non-discrimination (Article 14, ECHR).

---

[42] Bert-Jaap Koops, The concept of function creep, Law, Innovation and Technology Volume 13, 2021 - Issue 1, 16 Mar 2021, https://www.tandfonline.com/doi/full/10.1080/17579961.2021.1898299
[43] Lara Vomfell and Neil Stewart, Officer Bias, Over-Patrolling and Ethnic Disparities in Stop and Search, *Nature Human Behaviour,* 18 January 2021, https://warwick.ac.uk/fac/cross_fac/copr/news-events/stop-search/
[44] Christiane Wendehorst and Yannic Duller, Recognition and Behavioural Detection, *Policy Department for Citizens' Rights and Constitutional Affairs*, August 2021, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf
[45] Article 19, Emotional Entanglement: China's emotion recognition market and its implications for human rights, January 2021, https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf
[46] Ibid.
[47] Luuk Ex, Bo Hijstek and Mariëtte van Huijstee, Human Rights Risks from Immersive Technologies, *Business and Human Rights Journal*, 3 October 2025, https://www.cambridge.org/core/journals/business-and-human-rights-journal/article/human-rights-risks-from-immersive-technologies/79C8298E2246BD47A6E9F6EED982D55E#fn16

The technology also raises privacy concerns by making assumptions about individual's thoughts or intentions, which if inaccurately reflected could also bear further consequences (Article 8, ECHR). Claims that emotion recognition technology can infer people's 'true' inner states, and making decisions based on these inferences also has implications for freedom of expression (Article 10, ECHR).[48]

Overall, inferential technologies can never meet the narrowly defined tests of legality, necessity and proportionality. The legal framework should therefore prohibit the use of inferential technologies due to the risk to human rights.

1.1.6. The use of FRT at protests

Considering question 7 of the consultation PI recommends that the new legal framework includes restrictions as to how law enforcement use FRT and other biometric technologies at protests. This includes that they shall not be used to identify protesters or to collect information on people attending protests to ensure compliance with rights such as the right to freedom of association, expression and assembly under Articles 9, 10 and 11 of the ECHR.

In *Glukhin v. Russia* the ECtHR examined the use of FRT to identify and track down a protester who held an individual demonstration in the Moscow underground, eventually leading to his arrest.[49] The police took screenshots of photos and a video of the protester's demonstration from social media, as well as collecting footage from CCTV installed in the stations of the Moscow underground, and several days later, used live FRT to locate and arrest him while he was traveling in the underground. The Court unanimously found that Russia violated Article 8 and Article 10 of the ECHR.[50]

The UN Special Rapporteur on freedom of assembly and of association has also provided comment on the use of surveillance technologies at protests, including that "surveillance against individuals exercising their rights of peaceful assembly and association can only be conducted on a targeted basis, where there is a reasonable suspicion that they are engaging in or planning to engage in serious criminal offences, and under the very strictest rules, operating on principles of necessity and proportionality and providing for close judicial supervision" and hence recommended that "indiscriminate and untargeted surveillance" both online and offline should be outlawed.[51]

Furthermore, the UN High Commissioner for Human rights has also stated technology-enabled surveillance has been a major factor in the shrinking of civic space and there should be a

[48] Article 19, Emotional Entanglement: China's emotion recognition market and its implications for human rights, January 2021, https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf
[49] *Glukhin v. Russia*, Application no. 11519/20, 4 July 2023. https://hudoc.echr.coe.int/#{%22itemid%22:[%22001-225655%22]}
[50] Ibid.
[51] Report of the United Nations High Commissioner for Human Rights: Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests, A/HRC/44/24, 24 June 2020.

moratorium on the use of facial recognition technology in the context of peaceful protests, until States meet certain conditions including human rights due diligence before deploying it.[52]

1.7 Provisions concerning training and impact assessments

Training

Any law enforcement body using biometric technologies must have completed training, which will be updated annually. This training should focus on how to use the relevant system; on assessing the human rights impacts of the use of the system; how to determine whether the use is strictly necessary and proportionate; and how to fully comply with the law underpinning the use of biometric technologies.[53]

Impact Assessments

The Court of Appeal previously found that South Wales Police had failed to carry out a proper data protection impact assessment (DPIA); and that they had failed to comply with the public sector equality duty in section 149(1) Equality Act 2010 with regards to their use of LFRT.

PI recommends that the legal framework outlines a duty for law enforcement bodies that plan to deploy biometrics technologies, including FRT, to conduct human rights, data protection and equality impact assessments prior to the first deployment of new biometrics systems. These assessments must include, but not be limited to, an assessment of the impact on ECHR rights including an assessment of the strict necessity and proportionality requirements, and to prevent and mitigate unlawful discrimination, including indirect discrimination.

4. Reference Databases (In response to questions 12 and 13)

The use of databases, including Government databases, for FRT poses several risks. First, Conducting FRT searches against biometric or other personal data derived from a database constitutes an ongoing interference with the right to a private and family life under Article 8 of the ECHR.[54] It interferes with the rights of anyone whose personal data is processed, or at risk of being processed, to ascertain their identity, or to evaluate whether they are the person in a probe image.[55] Second, the legitimacy, quality and accuracy of the images in the database may be compromised. Images may be sourced unlawfully, for example through scraping a social media site, or gathered from a leak. The source and quality of the images impact the accuracy of a search and may result in misidentification. Third, a database may be developed through discriminatory practices, and its onward use may reinforce such discrimination. For example, a police database may contain a disproportionately high number of black people due to historic over-policing. This means innocent people from certain groups are more likely

---

[52] Office of the High Commissioner for Human Rights, New technologies must serve, not hinder, right to peaceful protest, Bachelet tells States, 25 June 2020, https://www.ohchr.org/en/press-releases/2020/06/new-technologies-must-serve-not-hinder-right-peaceful-protest-bachelet-tells
[53] Ibid. at 49.
[54] See: *R (Catt) v ACPO* [2015] AC 1065, [6]; *S & Marper v United Kingdom* (2009) 48 EHRR 50, [67], [77] and [86]
[55] See by analogy *R (Bridges) v Chief Constable of South Wales Police* [202] 1 WLR 672 (DC)[55]-[62]

to be flagged by the system. Fourth, data contained in a database is typically collected and processed for a purpose that the data subject has either consented to or is at least aware of. To repurpose the database and further process it in ways that may be incompatible with the original purpose, and without the consent or awareness of the data subject, may undermine data protection principles.

An interference with the right to a private and family life under Article 8 of the ECHR cannot be lawful unless it satisfies the requirements of Article 8(2) of the ECHR. Specifically, the interference must be in pursuit of a legitimate aim, be in accordance with the law, and necessary in a democratic society.

For an interference to be in accordance with the law, it must have a basis in domestic law and be compatible with the rule of law. Compatibility with the rule of law requires compliance with the requirements of accessibility and foreseeability, and it must contain sufficient constraints against arbitrary or disproportionate use.[56] The ECtHR has held, in the context of a biometric database, that it is "essential…to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness."[57] Most crucially, the use of a database for FRT reference purposes must be necessary and proportionate. This requirement may not always be met, especially for databases which contain information on most of the population.

Accordingly, the use of any database should be authorised by law and require a robust proportionality assessment at the outset. The law should provide sufficient detail to the public about which databases may be used, and the circumstances and conditions under which they may be accessed. Specifically, the law should require and include details concerning:

1. An assessment of whether use of the database for the stated biometric surveillance purpose is necessary and proportionate.
2. The criteria used to assess whether a database is fit for purpose and may be used for FRT searches. This should include an assessment of the technical specs of the database including whether there are any data protection, discrimination or other human rights concerns. The oversight Body may be best place to evaluate whether a database is fit for purpose.
3. The procedure for prior judicial authorisation of the use of a database for a particular search;
4. Details about how the database is accessed (e.g whether law enforcement is given direct access to a database or whether a search is run by the database owner on behalf of law enforcement);
5. The safeguards in place to mitigate against any identified harms;
6. Usage;

---

[56] *R (Bridges) v Chief Constable of South Wales Police* [2020] 1 WLR 5037 (CA),[80].
[57] *S & Marper v United Kingdom* (2009) 48 EHRR 50 [99].

7. Storage;
8. Retention;
9. Access of third parties;
10. Procedures for preserving the integrity and confidentiality of data;
11. Procedures for destruction;
12. Oversight mechanisms, including the requirement to keep a record of the requests to access a database. The record should note whether the requests were accepted or rejected, and the reasons why.

We submit that access to and use of private databases by law enforcement should be prohibited. Such databases are often developed in violation of data protection laws, and there is limited oversight over the quality, accuracy, or rights-based compliance with these databases. Further, creating a financial incentive for the development of these databases has a chilling effect on people's willingness to express themselves online, and can be a threat to people going about their lives freely.[58] The recent controversies around the Clearview[59] and PimEyes[60] databases highlight the concerns and risks of using private databases.

6. Independent Oversight body (In response to questions 14 & 15)

An independent oversight body should be established to ensure FRT, and other biometric technologies are deployed responsibly and in compliance with the law.

Such a body should be independent in structure and function. This requires structural independence from both the executive as well as the law enforcement bodies it oversees.[61] Functional independence requires that consideration be given to operational factors such as resources and budget, terms of office, rules on conflicts of interest and appointment processes.[62] These components are critical to independence as they allow oversight bodies to make difficult or unpopular decisions without fear of losing their jobs, or resources.[63]

The establishment, role, powers and obligations of the body should be clearly set out in primary legislation. Importantly, the law should also clearly identify which technologies and bodies it has oversight over.

---

[58] Privacy International, 'Get out of our face, Clearview!' https://privacyinternational.org/campaigns/get-out-our-face-clearview
[59] Privacy International, 'Get out of our face, Clearview!' https://privacyinternational.org/campaigns/get-out-our-face-clearview
[60] Privacy International, 'Joint letters to the Information Commissioner and Commissioner of the Metropolitan Police on use of PimEyes' https://privacyinternational.org/advocacy/5350/joint-letters-information-commissioner-and-commissioner-metropolitan-police-use
[61] Szabó v. Hungary, App. No. 37138/14, ¶ 77 (Jan. 12, 2016), see also Big Brother Watch v. United Kingdom, App. Nos. 58170/13, 62322/14, & 24960/15
[62] Darragh Murray, Peter Fussey, LornaMcGregor and Maurice Sunkin 'Effective Oversight of Large-Scale Surveillance Activities: A Human Rights Perspective; https://repository.essex.ac.uk/30085/5/Effective_Oversight_of_Large_Scale_Surveillance_Activities.pdf page 7.
[63] Tara Davis, 'Data Protection in Africa: A Look at OGP Member Progress', https://www.opengovpartnership.org/wp-content/uploads/2021/08/OGP-Data-Protection-Report.pdf page 8.

The ECtHR has considered the requirements of effective oversight in the context of surveillance and held that an oversight body should be able to "exercise an effective and continuous control."[64] To do so, it must be appropriately empowered to assess all elements of the deployment of FRT and conduct investigations and assessments. Given the technical nature of the deployment of FRT, coupled with the complex rights-based questions it poses, such an assessment requires the body to be resourced with a range of subject-matter experts.[65]

Importantly, the independent body should be empowered and equipped to hear and respond to complaints from members of the public. The law should accordingly empower the body to receive, investigate, and resolve complaints. This requires that the body be authorised to access the necessary information, including the power to compel disclosure, and enforce remedies. The law should establish a complaints procedure and provide for appropriate remedial actions or penalties the body may impose.

Importantly, if the oversight body is empowered to receive complaints, its role in all elements of the deployment of FRT needs to be carefully considered. Specifically, whether it should be involved at the authorisation phase, during deployment, and during post-facto review.[66] If one body is involved in all three phases, it is tantamount to "marking your own homework."[67] We accordingly submit that the oversight body should not be involved at the authorisation phase – and this should instead be conducted by a judicial commissioner or other judicial body.

Finally, the oversight body should be required to report to the public and parliament annually about its work and findings.

Additional matters

Standards regarding the quality of data including tests for accuracy and racial bias (In response to questions 16 & 17)

There is strong evidence that biometric technologies including FRT can have discriminatory results particularly for women, black people and other ethnic minorities which has implications for compliance with Article 14 ECHR. Research from MIT Media Lab revealed that facial recognition systems contain gender and racial biases that increase the likelihood of errors in identifying non-white individuals, particularly Black women.[68] This can lead to serious

---

[64] See Zakharov v. Russia, App. No. 47143/06, 233 (Dec. 4, 2015)
[65] Darragh Murray, Peter Fussey, Lorna McGregor and Maurice Sunkin 'Effective Oversight of Large-Scale Surveillance Activities: A Huamn Rights Perspective; https://repository.essex.ac.uk/30085/5/Effective_Oversight_of_Large_Scale_Surveillance_Activities.pdf page 7.
[66] Darragh Murray, Pete Fussey, Lorna McGregor and Maurice Sunkin, 'Effective Oversight of Large-Scale Surveillance Activities: A Huamn Rights Perspective; https://repository.essex.ac.uk/30085/5/Effective_Oversight_of_Large_Scale_Surveillance_Activities.pdf page 15.
[67] Ibid. pg 10.
[68] Larry Hardesty, Study finds gender and skin-type bias in commercial artificial-intelligence systems, *MIT News Office*, 11 February 2018, https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212

consequences, such as failure to correctly identify individuals, stigmatisation in public spaces and even lead to wrongful arrest and detention, risks that will only be exacerbated for marginalised communities.

We have already experienced instances of misidentification through the police's use of FRT in the UK. In May 2024, Shaun Thompson, an anti-knife crime youth worker was misidentified by the Met during a LFRT deployment at London Bridge. As a result, a judicial review has been taken against the force's use of LFRT. Furthermore, it has been reported that between September 2024 and September 2025 the Met's use of LFRT saw 80% of people who were falsely alerted were black.[69] What is even more concerning is that these racial inaccuracies were confirmed by the National Physical Laboratory (NPL) in 2024.[70]

Law enforcement bodies should be informed in prior training of the risks of racially and otherwise discriminatory outcomes of FRT. The proposed new oversight body could outline specific rules for law enforcement organisations to follow to guard against bias and discrimination when using FRT. Including specifications to consider in an impact assessment before deployment. As well as have oversight of the type of FRT software being used by law enforcement, to ensure standards regarding the quality of data including tests for accuracy and racial bias. If it is identified that they pose too grave a risk, and where concerns of discrimination cannot be mitigated, it should not be deployed.

Application of the legal framework beyond law enforcement (In response to question 5)

PI recognises that the intention is that the new legal framework will apply to the law enforcement bodies listed within the consultation only. We submit that the framework should extend its scope to the use of biometric technologies that are deployed by non-law enforcement bodies but are used for law enforcement purposes.

We also recommend that the legal framework should extend to Local Authorities. Video surveillance systems, including automatic number plate recognition (ANPR) and CCTV systems, are operated by most Local Authorities in England and Wales and are intrinsically linked with operational policing.[71] Local authorities are also seeking to use AI and new technologies, including to upgrade CCTV cameras to be integrated with FRT. Hammersmith and Fulham Council have already revealed potential plans for an extensive expansion of FRT across the West London borough.[72] The Council's Cabinet White Paper sets out details to introduce new

[69] Jess Warren, No arrests from false facial recognition alerts, *BBC News,* 31 October 2025, https://www.bbc.co.uk/news/articles/c4gp7j55zxvo
[70] Daniel Boffey and Mark Wilding, 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
[71] Tony Porter, Blog: How effective are Video Surveillance Systems (VSS)? Surveillance Camera Commissioner's Office, 28 May 2019, https://videosurveillance.blog.gov.uk/2019/05/28/how-effective-are-video-surveillance-systems-vss/
[72] Ben Lynch, Council to introduce facial recognition CCTV, *BBC News*, 18 September 2025, https://www.bbc.co.uk/news/articles/crl5030lwkwo

static LFRT "cameras which match faces against a defined police database in real time, with police on standby to engage with matched individuals".[73] These are to be installed at identified crime hotspots at 10 locations across the borough, with two cameras initially trialed at each of the 10 locations.[74] Five hundred existing cameras will also be upgraded with AI capabilities to enable RFRT.

PI has also been monitoring the increasing rise of the private sector utilising FRT. Private sector entities including banks, supermarkets, nightclubs, gyms, and more have increasingly adopted FRT for purposes such as age verification, crime prevention, access control, and workplace monitoring.[75] Several UK retailers and supermarkets across the UK including Asda[76], Sainsbury's[77], Iceland[78], Home Bargains[79], and others have been using FRT in their stores. Furthermore, their use of FRT has already led to several cases of misidentification of shoppers who have subsequently been refused entry.[80] Some of these businesses are using software provided by Facewatch[81] who's practices raise data protection concerns.[82] These deployments operate with minimal transparency and oversight, potentially discriminating against marginalised communities with lower-income areas disproportionately targeted.[83]

The private sector is subject to the Data Protection Act (DPA) 2018, which we maintain should prohibit the private sector from using these technologies. However, the Information Commissioners Office (ICO) who oversees their compliance with the DPA have yet to take sufficient action. Although the proposed framework would not encompass the private sector's use of FRT, we recommend that further action is taken by the government to address these gaps and the private sector's unlawful use of FRT.

---

[73] London Borough of Hammersmith & Fulham Council Report, White Paper: 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 and Artificial Intelligence.pdf

[74] Ibid.

[75] Julie Zagg, London's use of facial recognition is surging, despite technology's flaws, *Le Monde*, 19 January 2025, https://www.lemonde.fr/en/economy/article/2025/01/19/london-s-use-of-facial-recognition-is-surging-despite-technology-s-flaws_6737187_19.html

[76] Ali Nassar-Smith, Privacy Groups Challenge Asda's Facial Recognition Trial in UK Stores, *ID Tech,* 22 May 2025,

[77] Kevin Rawlinson, 'Orwellian': Sainsbury's staff using facial recognition tech eject innocent shopper, The Guardian, 5 February 2025, https://www.theguardian.com/technology/2026/feb/05/london-man-sainsburys-facial-recognition-facewatch

[78] Paul Kunert, Frozen foods supermarket chain deploys facial recognition tech, *The Register,* 26 June 2025, https://www.theregister.com/2025/06/26/iceland_facial_recognition/

[79] James Clayton, 'I was misidentified as shoplifter by facial recognition tech', *BBC News*, 26 May 2024, https://www.bbc.co.uk/news/technology-69055945

[80] Kateryna Pavlyuk, Sainsbury's ejects man misidentified as offender, *BBC News*, 5 February 2026, https://www.bbc.co.uk/news/articles/c0lxdn4w2g3o

[81] See: https://www.facewatch.co.uk/

[82] Big Brother Watch, Update: Big Brother Watch's complaint to the ICO on retailer facial recognition, 28 June 2023, https://bigbrotherwatch.org.uk/blog/update-big-brother-watchs-complaint-to-the-ico-on-retailer-facial-recognition/

[83] Shanti Das, Facial recognition cameras in supermarkets 'targeted at poor areas' in England, *The Guardian*, 27 January 2024, https://www.theguardian.com/uk-news/2024/jan/27/facial-recognition-cameras-in-supermarkets-targeted-at-poor-areas-in-england

PI is supported in this submission by Glitch.[84] Glitch is a digital rights and tech policy charity that looks at these issues from a racial and gender justice lens. Glitch notes their particular concern with the wider context of racism and discrimination that police use of FRT operates within, and disagrees with the Government's use of violence against women and girls (VAWG) as justification for further investment into FRT.[85]

[84] See: https://glitchcharity.co.uk/
[85] Glitch, Government VAWG Strategy - Our Response, 8 January 2026, https://glitchcharity.co.uk/blog/vawg-strategy-response