

BIG BROTHER WATCH

Big Brother Watch Submission to UK Government Consultation on a new legal framework for law enforcement use of biometrics, facial recognition and similar technologies

Contents

1. Which technologies should the legislative framework cover? [[Q1-4](#)]
2. Which organisations should fall within the scope of the legislative framework? [[Q5](#)]
3. When should law enforcement organisations be allowed to use these technologies? [[Q6-9, 12-13](#)]
4. Authorisation and oversight [[Q10-11, 14-17](#)]

Executive summary

Big Brother Watch welcomes the opportunity to respond to the Home Office's Consultation on a new legal framework for law enforcement use of biometrics, facial recognition, and similar technologies. Facial recognition technologies (FRT) have proliferated across police forces and the private sector despite any specific legislation governing their use. Given the intrusive nature of FRT, increasing adoption of biometric and inferential technology, and the government's plans to ramp up police FRT deployments, the consultation is especially urgent.

Our response will explain why the legal framework is required and how it should apply to live facial recognition (LFR), retrospective facial recognition (RFR), operator initiated facial recognition (OIFR), other biometric technologies and increasingly common inferential technologies. It will also argue that the framework should cover both law enforcement and private uses of these technologies.

Left unchecked, FRT threatens to underpin a mass surveillance infrastructure across every "city, town and village"¹ in the UK, which has the capacity to indiscriminately track, monitor, and identify citizens as they go about their daily lives. As a colonel in the Gendarmerie in France explained, this technology is powerful because it makes "this control invisible" in a system in which "identity checks would be permanent and universal."² Home Secretary Shabana Mahmood seems to share this vision for the country. In recent remarks she explained that her aim is "to achieve, by means of AI and technology, what Jeremy Bentham tried to do with his Panopticon. That is that the eyes of the

¹ The Telegraph, Live facial recognition cameras planned for every town centre, 4 December 2025, <https://www.telegraph.co.uk/politics/2025/12/04/live-facial-recognition-cameras-planned-for-every-town-cent/>.

² La Quadrature du Net, In France, the eternal return of facial recognition, 4 September 2025, <https://www.laquadrature.net/en/2025/09/04/in-france-the-eternal-return-of-facial-recognition/>.

state can be on you at all times.”³ FRT is an ideal tool for such a vision and left unchecked, it threatens to irreversibly diminish our ability to exist freely in publicly-accessible spaces.

Over the past decade, police have been experimenting with FRT absent any specific law governing the technology. The result has been years of controversy. The use of FRT by police forces across the UK has been plagued with secrecy, inaccuracies, racial bias,⁴ misidentifications,⁵ deployment at protests,⁶ and the targeting of individuals with mental health problems.⁷ A reliance on a patchwork of human rights, data protection and equalities law has led to police forces adopting overly broad and permissive policies that have been the subject of legal challenge. The UK stands alone among other liberal democracies in allowing the widespread use of FRT absent controls. Given this history and the nature of FRT, the new legislative framework should be subject to strict controls and regulations.

Given the threats to fundamental rights posed by FRT we make the following recommendations:

- 1) The new legislative framework should adopt a broadly prohibitive approach, allowing FRT in only strictly defined circumstances and using the EU AI Act model as a baseline for regulation.
- 2) The use of FRT by non-law enforcement bodies must be included within the scope of the new legislative framework.

Introduction

The consultation is welcome, but it is also long overdue. Big Brother Watch has been investigating and reporting on the expansion of intrusive FRT since police trials of LFR publicly began in 2016.⁸ Despite the serious accuracy and legal issues, ten police forces currently own LFR technology and deploy it on a regular basis. In Croydon, the Metropolitan Police have already experimented with a

³ The National Scot, Shabana Mahmood proposes AI 'Panopticon' system of state surveillance, 20 January 2026, <https://www.thenational.scot/news/25780001.shabana-mahmood-proposes-ai-panopticon-system-state-surveillance/>.

⁴ Liberty Investigates, 'UK police forces lobbied to use biased facial recognition technology,' 10 December 2025, <https://libertyinvestigates.org.uk/articles/police-forces-biased-facial-recognition-technology/>; Interim report of the Biometrics and Forensics Ethics Group Facial Recognition Working Group, February 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/781745/Facial_Recognition_Briefing_BFEG_February_2019.pdf; BBC News, 'Biased and wrong? Facial recognition tech in the dock,' 8 July 2019, https://www.bbc.co.uk/news/business-48842750?intlink_from_url=&link_location=live-reporting-story.

⁵ BBC News, 'Facial recognition tech mistook me for wanted man,' 6 August 2025, <https://www.bbc.co.uk/news/articles/cqxg8v74d8jo>.

⁶ BBC News, 'Facial recognition: What led Ed Bridges to take on South Wales Police?' 11 August 2020, <https://www.bbc.co.uk/news/uk-wales-53742099>; BBC News, 'F1 British Grand Prix: Facial recognition at Silverstone being used,' 6 July 2023, <https://www.bbc.co.uk/news/uk-england-northamptonshire-66120010>.

⁷ The Guardian, 'Police to use facial-recognition cameras at Cenotaph service,' 12 November 2017, <https://www.theguardian.com/technology/2017/nov/12/metropolitan-police-to-use-facial-recognition-technology-remembrance-sunday-cenotaph>.

⁸ ITV News, 'Face recognition police to scan Notting Hill Carnival CCTV for offenders,' 28 August 2016, <https://www.itv.com/news/2016-08-28/face-recognition-police-to-scan-notting-hill-carnival-cctv-for-offenders>.

fixed LFR camera system, which appears to be set to stay. During this consultation's submission window the Home Secretary announced that the new National Police Service "will include the largest-ever roll-out of LFR technologies, across England and Wales"⁹ and the number of live facial recognition vans will increase five-fold.¹⁰ There is widespread concern that, no matter what the views of stakeholders and indeed the public may be, rapid and significant expansion of LFR is a fait accompli.

Whilst specific legislation governs the controls and oversight of other forms of biometric processing, such as DNA and fingerprinting, FRT has proliferated in the UK without any primary legislation. Instead, police have relied on data protection, human rights, and equalities law as a patchwork legal backdrop for their use of FRT – laws that were not written with FRT in mind and that do not contain any specific provisions on FRT at all. Police forces rely on general common law powers as the legal basis for their use of FRT, while non-law-enforcement bodies such as retail outlets are constrained only by the largely unenforced requirements of data protection legislation.¹¹

The current state of the law is untenable. Police forces have different highly permissive standard operating policies, which have been subject to legal challenge. Numerous academics and think tanks, from the sociotechnical audit produced by the Minderoo Centre for Technology & Democracy at the University of Cambridge¹² to the Ada Lovelace Institute's independent legal review of the governance of biometric data in England and Wales¹³ have found that the existing legal position is not fit for purpose. The Lords Home Affairs and Justice Committee also called for a "legislative framework, authorised by Parliament for the regulation of the deployment of LFR technology."¹⁴

The new legislative framework would present an opportunity to rectify the situation. A strict statutory regime should govern FRT and similar technologies. Given the inherently intrusive nature of biometric technologies, this regulation must take the form of primary legislation that is subject to public debate and parliamentary scrutiny.

There is much to learn from the European Union's multi-year legislative process, recently resulting in the Artificial Intelligence Act (Regulation (EU) 2024/1689), commonly known as the "EU AI Act". Drawing on legal and technological expertise from across the continent, the EU AI Act imposes a general prohibition on real-time remote biometric identification owing to the high risk it poses to fundamental rights. Likewise, the first and most fundamental safeguard in the UK's new framework should be that the legislation is restrictive by default,

⁹ HC Deb, 26 January 2026, vol 779, col 610, <https://hansard.parliament.uk/commons/2026-01-26/debates/1D438294-73B0-4322-9E40-D5EEBD7702ED/PoliceReformWhitePaper>.

¹⁰ Gov.uk, 'White paper sets out reforms to policing,' 26 January 2026, <https://www.gov.uk/government/news/white-paper-sets-out-reforms-to-policing>.

¹¹ Data Protection Act 2018 and UK GDPR.

¹² University of Cambridge, 'UK police fail to meet 'legal and ethical standards' in use of facial recognition,' 27 October 2022, <https://www.cam.ac.uk/research/news/uk-police-fail-to-meet-legal-and-ethical-standards-in-use-of-facial-recognition>.

¹³ Ada Lovelace Institute, The Ryder Review: Independent legal review of the governance of biometric data in England and Wales, 2022, <https://www.adalovelaceinstitute.org/report/ryder-review-biometrics/>.

¹⁴ Letter from Chair, House of Lords Justice and Home Affairs Committee to Home Secretary regarding investigation into the use of LFR by police forces in England and Wales, 26 January 2024, <https://committees.parliament.uk/publications/43080/documents/214371/default/>.

ensuring that the deployment of biometric technologies are only used when strictly necessary and as such are the exception to day-to-day policing rather than the norm. Experience shows that in the absence of firm legal constraints law enforcement bodies and organisations deploy FRT in controversial ways. There is also a precedent of police forces deploying these technologies on a pilot or trial basis without adequate oversight or authorisation and subsequently retaining them.¹⁵ We cannot rely on post-hoc intervention by the ICO to curb experimental uses of biometric technologies given that its enforcement mechanisms have so far been ineffective.

1. Which technologies should the legislative framework cover? [Q1-4]

1.1 Facial recognition technology

The consultation does not distinguish between the use of LFR, RFR, and OIFR technologies. The rationale for this decision is that the legal framework will need to apply to all existing and possible use cases of FRT, recognising that the interference with individual rights will vary depending on a range of factors. However, the specific type of FRT used will affect the level of interference with individual rights.

Live facial recognition (LFR)

LFR poses a significant threat to the rights and freedoms of the population. Its use by police presents a radical departure from long-held principles embedded in UK policing practices that serve to protect our rights and freedoms. It is a fundamental principle that individuals should not have to identify themselves to the police unless they are suspected of criminal behaviour. LFR reverses this protection by indiscriminately subjecting innocent members of the public to mass identity checks without any suspicion of wrongdoing.

The deployment of LFR technology threatens privacy both on an individual level and as a societal norm. The AI-powered mass surveillance software takes biometric scans of each individual who passes by the camera and retains photos of those flagged by the system – even where no further action is taken by the police. The significance of a technology which subjects us all to constant surveillance that does not only record our whereabouts and activities but can also identify us in real-time as we go about our daily lives cannot be understated. Indiscriminate mass surveillance can never be a proportionate interference with human rights and has no place in a rights-respecting democracy. That makes LFR safeguards highly important to protect the public.

In recent years, parliamentarians across parties in Westminster,¹⁶ members of the Senedd,¹⁷ rights and equalities groups, and technology experts across the

¹⁵ Metropolitan Police Announcement, '100 arrests following new Live Facial Recognition pilot in Croydon,' 19 January 2026, <https://news.met.police.uk/news/100-arrests-following-new-live-facial-recognition-pilot-in-croydon-505225>.

¹⁶ The Guardian, MPs and peers call for 'immediate stop' to live facial recognition surveillance, 6 October 2023, <https://www.theguardian.com/technology/2023/oct/06/mps-and-peers-call-for-immediate-stop-to-live-facial-recognition-surveillance>.

¹⁷ Nation Cymru, Concerns raised about 'intrusive' use of live facial recognition technology, 20 December 2023, <https://nation.cymru/news/concerns-raised-about-intrusive-use-of-live-facial->

globe have called for a stop to the use of FRT.¹⁸ The Science and Technology Committee echoed the call, recommending an immediate moratorium on police use of LFR in 2019.¹⁹ Local councils in Haringey,²⁰ Newham,²¹ Islington²² and South Oxfordshire²³ have also passed symbolic motions calling for bans on FRT.

There is a clear need to legislate to restrain the use of LFR in the UK. LFR has been subject to two legal challenges in England and Wales. In 2019, the Court of Appeal found that South Wales Police's use of LFR was unlawful and had violated human rights, equalities, and data protection law.²⁴ In January 2026, the High Court heard the judicial review against the Metropolitan Police's LFR use brought by anti-knife crime community volunteer Shaun Thompson, who was misidentified by the technology and wrongly flagged as a criminal.²⁵ The Equality and Human Rights Commission has intervened in the challenge, arguing that the force's use of the technology is incompatible with human rights.²⁶

The EU AI Act singles out 'real-time' biometric technologies' (i.e., LFR) as requiring specific broad prohibitions, explaining that its use:

*"is particularly intrusive to the rights and freedoms of the concerned persons, to the extent that it may affect the private life of a large part of the population, evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights."*²⁷

Given the vast array of threats that LFR technology poses to human rights, coupled with its intrinsically disproportionate nature it should be explicitly prohibited in the UK. The new legislative framework should at a minimum align the UK's position with that of the rest of Europe under the EU AI Act.

[recognition-technology/](#).

¹⁸ Byline Times, Over 180 Rights Groups and Tech Experts Call for UK and Worldwide Halt to Facial Recognition Surveillance, 27 September 2023, <https://bylinetimes.com/2023/09/27/over-180-rights-groups-and-tech-experts-call-for-uk-and-worldwide-halt-to-facial-recognition-surveillance/>.

¹⁹ House of Commons Science and Technology Committee, 'Issues with biometrics and forensics significant risk to effective functioning of the criminal justice system,' 18 July 2019, <https://committees.parliament.uk/committee/135/science-and-technology-committee/news/100970/issues-with-biometrics-and-forensics-significant-risk-to-effective-functioning-of-the-criminal-justice-system/>.

²⁰ Haringey Council Motion, 19 March 2020, <https://www.minutes.haringey.gov.uk/mgAi.aspx?ID=64618>.

²¹ Computer Weekly, Newham Council rejects use of live facial-recognition tech by police, 19 January 2023, <https://www.computerweekly.com/news/252529364/Newham-Council-rejects-use-of-live-facial-recognition-tech-by-police>.

²² Islington Council Motion, 11 July 2024, <https://democracy.islington.gov.uk/documents/b15774/Second%20Despatch%2011th-Jul-2024%2019.15%20Council.pdf?T=9>.

²³ South Oxfordshire District Council Motion, 23 October 2025, <https://democratic.southoxon.gov.uk/mgAi.aspx?ID=20068>

²⁴ BBC, Facial Recognition use by South Wales Police ruled unlawful, 11 August 2020, <https://www.bbc.co.uk/news/uk-wales-53734716>.

²⁵ BBC, 'Facial recognition tech mistook me for a wanted man,' 6 August 2025, <https://www.bbc.co.uk/news/articles/cqyg8v74d8jo>.

²⁶ Equality and Human Rights Commission, 'Met Police's use of facial recognition tech must comply with human rights law, says regulator,' 20 August 2025, <https://www.equalityhumanrights.com/met-polices-use-facial-recognition-tech-must-comply-human-rights-law-says-regulator>.

²⁷ Article 32 of the EU AI Act.

Operator-initiated facial recognition (OIFR)

OIFR has the potential to reshape police encounters with members of the public, giving officers access to powerful on-demand mobile surveillance technology that uses our faces to unlock a vast array of records held about us. Whether at protests, on the roads, or during stops and searches police officers could, depending on the size of image reference libraries they use, have the ability to instantly identify people with whom they interact, regardless of whether those people are suspected of a crime. This risk is heightened by the government's plans to introduce a digital ID system, which could create population-wide biometrically linked databases containing vast amounts of personal information, further facilitating detailed and pervasive identification.

Only in exceptional cases can the use of OIFR meet the tests of being a necessary and proportionate interference with fundamental rights. Police officers in the UK have no "stop and account" powers, meaning they cannot require an individual to give their name, address, or any account of what they are doing in the area. Individuals are only required to identify themselves if they have been informed that they are suspected of committing an offence. In South Wales Police's current policy on OIFR the grounds for an OIFR scan, as with other police uses of FRT, go beyond suspected criminal activity and include nebulous categories of presenting "a risk of harm to themselves or others". This broad category gives police forces vast scope to utilise FRT in a range of non-crime related situations.

If people being sought by the police are known individuals present at known locations it is not clear that OIFR is strictly necessary when considering the availability of less intrusive alternative methods (spotter cards or super recognisers, for example). However, there is a risk that such a technology could be used widely and indiscriminately to scan individuals in the crowd. Such a use of the technology would entirely undermine the proportionality of its use as well as make it highly inefficient. Individuals can be identified at police stations if there is a lawful reason for their arrest.

Big Brother Watch found serious racial bias in South Wales Police's use of OIFR with non-white members of the public being almost four times as likely to be subjected to an OIFR scan than white people.²⁸ These statistics reflect other policing practices, such as fingerprint scanning and stop and searches, where people of colour are more likely to be subject to policing interventions and surveillance. There is also a significant risk of discrimination on the grounds of nationality, age, and mental health when using OIFR. South Wales Police states that an OIFR scan can be undertaken if an individual is unable to provide their details, meaning those who cannot speak English or who struggle to communicate with police officers due to their age or mental capacity will be far more likely to be subject to an OIFR scan. This two-tier approach to policing, where those with communication issues, or disabilities are subject to intrusive facial scans at a higher rate, absent strict necessity, is deeply troubling and discriminatory. The impacts of unleashing OIFR on the public can be seen in the United States, where Immigration and Customs Enforcement agents have been

²⁸ Big Brother Watch, 'Biometric Britain' Report, 23 May 2023, p58.

using the technology to identify individuals as they are going about their daily lives in order to determine their immigration status.²⁹

1.2 Other biometric technologies

1.2.1 Need for regulation

Other biometric technologies, such as voice and iris recognition and inferential technologies must be included in the legislative framework. As Big Brother Watch has documented in recent years, the public and private sector are increasingly using biometric and AI-powered surveillance. Gait analysis, emotion detection, and age, gender, and ethnicity recognition software is being advertised and installed across the UK despite concerns about this technology's accuracy, bias, efficacy, and impact on our fundamental liberties. In his annual 2024 report, former Biometrics and Surveillance Camera Commissioner Tony Eastaugh identified emerging technologies based on voice patterns, odour, and gait as areas requiring increased policy attention and regulatory oversight.³⁰

The EU AI Act adopts a restrictive approach to these technologies by banning AI systems that infer emotions in workplaces and educational settings, prohibiting predictive or risk-based assessments of criminal behaviour without specific suspicion, and restricting the use of biometric categorisation systems outside law enforcement.³¹ Given the proliferation of these technologies, the new legislative framework should take a similarly prohibitive approach. This would offer an opportunity to establish meaningful safeguards around their use, as well as providing clarity to software developers.

1.2.2 Inferential technologies

Private companies are already experimenting with inferential technologies. Developers of these technologies claim they can deduce people's inner states, behaviours, and characteristics despite evidence that these systems often rely on pseudo-scientific assumptions.³² Big Brother Watch uncovered that between 2022 and 2024 eight train stations across the UK trialled Amazon's AI surveillance software with their CCTV cameras to analyse passengers' age, gender, and emotions.³³ Some firms are using similar products during recruitment to analyse candidates' behaviour, speech, and tone.³⁴ Other

²⁹ NPR, Immigration agents have new technology to identify and track people, 8 November 2025, <https://www.npr.org/2025/11/08/nx-s1-5585691/ice-facial-recognition-immigration-tracking-spyware>.

³⁰ Biometrics and Surveillance Camera Commissioner, 2023-2024 Annual Report, 2 December 2024, <https://www.gov.uk/government/publications/biometrics-and-surveillance-camera-commissioner-report-2023-to-2024/biometrics-and-surveillance-camera-commissioners-annual-report-2023-to-2024-accessible>.

³¹ Articles 5(d), (f) and (g).

³² Ada Lovelace Institute, 'An Eye on the Future: A Legal Framework for the governance of biometric technologies in the UK' Report, 29 May 2025, <https://www.adalovelaceinstitute.org/report/an-eye-on-the-future/>.

³³ Wired, Amazon-Powered AI Cameras Used to Detect Emotions of Unwitting UK Train Passengers, 17 June 2024, <https://www.wired.com/story/amazon-ai-cameras-emotions-uk-train-passengers/>.

³⁴ The Telegraph, 'AI used for first time in job interviews in UK to find best applicants', 27 September 2019, <https://www.telegraph.co.uk/news/2019/09/27/ai-facial-recognition-used-first-time-job-interviews-uk-find/>.

software developers are creating tools that track subconscious emotional responses for marketing and advertising purposes, boasting that they could also be used for identifying financial fraud, psychological evaluations, lie detection, and workplace surveillance.³⁵

1.2.3 Other biometric technologies

Where real-time biometric technologies are used in publicly accessible spaces, they may engage the same concerns as LFR, such as enabling remote identification or tracking without the consent or knowledge of the subject. Researchers are rapidly developing gait and cardiac recognition software to identify people by their walk and even their heart rhythms.³⁶ As such, they should be restricted by default or at the very minimum mirror the restrictions of real-time biometric surveillance under the EU AI Act.

There is also a need for strict regulation governing where and why other biometric technologies are used retrospectively. In 2019, the National Crime Agency was reportedly covertly creating a database of audio voice recordings to identify suspects by their unique voiceprint.³⁷ Several companies are also piloting projects for identifying individuals by their unique chemical odour and the shape of their ear or their walk. These pilots are occurring at a time when it is already possible to identify someone using their palm prints and vein distribution.³⁸ Whilst some of these technologies may have a limited role to play in law enforcement, subject to robust testing, transparency requirements, and oversight this should not take place without a public debate about the necessity and proportionality of their use.

2. Which organisations should fall within the scope of the legislative framework? **[Q5]**

The new legal framework should apply to all uses of FRT and similar technologies, irrespective of the organisation using it or the purpose for which it is used. FRT has proliferated across the public and private sectors, with police often approving non-police deployments, which often act with few restrictions. Given the expansion of FRT and the ease with which it can be adopted, it threatens to become ubiquitous and remove anonymity in publicly accessible spaces. Failing to regulate non-law enforcement uses of FRT and other biometric technologies in the new legislative framework would be a missed opportunity with dangerous consequences.

³⁵ The Telegraph, The British companies pioneering AI that reads your emotions - and will revolutionise everything from shopping to sport, 30 May 2019, <https://www.telegraph.co.uk/technology/2019/05/30/british-companies-pioneering-ai-reads-emotions-will-revolutionise/>.

³⁶ The Telegraph, Think facial recognition is creepy? Soon your heartbeat or the way you walk could reveal your identity, 29 September 2019, <https://www.telegraph.co.uk/technology/2019/09/29/tech-can-identify-walk-heartbeat-way-hold-phone/>.

³⁷ Daily Mail, Britain's FBI secretly builds 'voiceprint' recordings database to catch crooks and could even get data from Alexa, 15 September 2019, <https://www.dailymail.co.uk/news/article-7464795/Britains-FBI-secretly-builds-voiceprint-recordings-database-catch-crooks.html>.

³⁸ The i Paper, How your walk and body odour could soon be used to track your every move, 18 January 2025, <https://inews.co.uk/news/how-walk-body-odour-track-every-move-3484876>.

The most effective way to regulate FRT and similar technologies is to introduce broad prohibitions for the mass use of these technologies in publicly accessible spaces, reflecting Chapter II of the EU AI Act, which includes tightly restricted exceptions for the limited appropriate use cases.

Leaving non-law-enforcement uses of FRT outside the scope of the new legislative framework would create an uneven regulatory landscape. The government sets out its position in the consultation that if non-law enforcement organisations are excluded from the scope of the new legal framework, they will still be required to comply with existing data protection law. However, as data protection legislation applies to both the private and public sectors, the same would be true of police forces uses of FRT. It would produce a perverse outcome if the law imposed stricter regulations for law-enforcement uses than private sector uses of the same technology when the privacy, discrimination and equality risks are comparable. Indeed, it is all the more important as private sector companies are not subject to the Human Rights Act in the same way as public bodies. It is necessary to provide legislative clarity for all uses of FRT.

We maintain that UK GDPR already generally prohibits private sector use of non-consensual facial recognition surveillance for illegitimate purposes, such as low-level crime/loss prevention, such as that deployed by retailers and platforms like PimEyes, which is an interpretation adopted by the European Data Protection Board³⁹ and enforced by European data regulators.⁴⁰ However, this has not prevented the expansion of live facial recognition in supermarkets and shops around the UK. Unfortunately, the Information Commissioner's Office (ICO) has been slow to intervene and in some cases has simply failed to intervene. The new legislative framework represents an opportunity to explicitly ban mass uses of FRT and similar technologies by non-law enforcement organisations in publicly accessible spaces for any purposes.

2.1 Non-law enforcement organisations using FRT

2.1.1 Public bodies

Given the intrusive nature of FRT, it should only be used by appropriately trained police or intelligence officers. We should not allow a broad range of actors, without the resources or remit to conduct criminal investigations, to deploy FRT.

It is difficult to imagine circumstances in which it would be strictly necessary and proportionate for public bodies such as the Environment Agency or HMRC to use any form of FRT for law enforcement purposes, given that their organisational remit does not extend to day-to-day law enforcement or public order policing. Where biometric identification is deemed necessary, this function

³⁹ European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices, Version 2.0, 29 January 2020, para 77, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf.

⁴⁰ Spanish DPA Fines Supermarket Chain 2,520,000 EUR for Unlawful Use of Facial Recognition System, Hunton Andrew Kirths, 30th July 2021, accessed 5th December 2024, <https://www.huntonak.com/privacy-and-information-security-law/spanish-dpa-fines-supermarket-chain-2520000-eur-for-unlawful-use-of-facial-recognition-system>; European Data Protection Board, 'Dutch Supervisory Authority imposes a fine on Clearview because of illegal data collection for facial recognition,' 3 September 2024, https://www.edpb.europa.eu/news/national-news/2024/dutch-supervisory-authority-imposes-fine-clearview-because-illegal-data_en.

should only be exercised by appropriately mandated law enforcement agencies that investigate crime of sufficient seriousness and that could meet a strict necessity test, rather than delegated to bodies without an explicit policing responsibility.

Local councils are also experimenting with the implementation of FRT technologies. In September 2025, Hammersmith and Fulham Council Cabinet approved plans for a £3.2 million investment in live and retrospective facial recognition, AI-assisted cameras, and drones for tackling crime and anti-social behaviour.⁴¹ Whilst there may be a case for police forces being able to temporarily use local councils' CCTV networks, provided the other requirements for FRT deployment are met, they must not be constantly accessible to law-enforcement bodies simply for the purpose of operating FRT – such activity would result in the type of generic mass surveillance that a legal framework should aim to prevent in a democracy. Further, the new legislative framework should explicitly prohibit the use of FRT by non-law enforcement bodies to prevent local authorities from expansively deploying intrusive technologies for low-level crime and monitoring of anti-social behaviour in conjunction with the police, albeit without being subject to the same rigorous restrictions as law-enforcement bodies. The threshold to use FRT must be high, commensurate with the high risk posed to millions of people's rights.

There is frequently a blurring of the lines between the use of FRT by law enforcement and non-law enforcement organisations. The police have deployed FRT, or approved its use, at a number of busy publicly accessible but privately owned places. In Granary Square, near Kings Cross Station in London, the private company that maintains the space had a secret photo-sharing agreement with the Met Police that that was in place for two years. Similarly, Greater Manchester Police secretly operated LFR at the UK's third largest shopping centre, the Trafford Centre, for six months in 2018. Under these schemes, police provided the images of individuals who they were looking for and the private companies alerted them when they obtained a match. In 2019, a Big Brother Watch investigation found several more instances of facial recognition being used at privately owned sites, including Meadowhall shopping centre in Sheffield, Millennium Point in Birmingham, and Liverpool's World Museum. These examples demonstrate the ease with which law enforcement agencies can appropriate non-law enforcement agencies to conduct FRT searches for their purposes and would allow any private camera feed in practice to be used for the purposes of FRT. These public-private partnerships using FRT must be prohibited under the new legal framework; third parties should not have access to FRT.

2.1.2 Private actors

FRT is currently used by a range of private actors for quasi-law enforcement purposes. We maintain that UK GDPR already prohibits private sector use of low-level surveillance using LFR software provided by firms such as Facewatch. However, despite these restrictions under data protection law, dozens of retailers across the UK are using or piloting live facial recognition technology in their shops. These include major supermarkets such as Asda, Sainsbury's, and

⁴¹ London Borough of Hammersmith & Fulham Council Report, 'CCTV and Artificial Intelligence – new innovations and improved infrastructure to help combat crime and anti-social behaviour,' 15 September 2025, <https://democracy.lbhf.gov.uk/documents/s132480/CCTV%20and%20Artificial%20Intelligence.pdf>.

Iceland as well as retailers such as B&M, Home Bargains, and Sports Direct. Facewatch boasts that more than 125 businesses are using their software.⁴²

Facewatch operates a subscription business, allowing individual retailers to add members of the public whom they wish to exclude from a store to a tailored watchlist, which generally comprises of images taken from customers' previous visits to a store. The AI-powered mass surveillance software indiscriminately captures the biometric information of each customer who passes by cameras. When individuals on the watchlist enter the store they are identified by FRT software and the staff are alerted to their presence. FRT software companies also offer 'National Watchlists' comprised of uploads of images and reports of crime and disorder submitted by their customers across the UK. As a result, if an individual is blacklisted from one of Facewatch's stores they can also be excluded from the stores of all their other clients in a set geographic radius. The FRT system retains photos of those flagged by the software – even if no police report is made or where no action is taken by the police, as per the vast majority of cases.

Retail use of LFR emboldens staff members to make criminal allegations against customers without an investigation or any set standard of proof and ban them from other stores employing the software. When errors are made this has profound implications for the lives of the accused, with little recourse for challenging the accusations. Individuals are required to submit more personal identifying data just to find out what they stand accused of. The lack of oversight, training and safeguards means that vulnerable individuals and minoritised groups are particularly at risk of being included on watchlists due to stereotypes, leaving the door open to discriminatory and unfair decisions.

In July 2022, Big Brother Watch filed a legal complaint to the ICO in relation to Southern Co-op's use of Facewatch's LFR technology in its stores. The ICO launched an investigation into Facewatch which concluded in 2023. Its investigation found that the company's policies breached data protection law as they "failed to balance the legitimate interest of Facewatch and their subscribers against the rights and freedoms of individuals."⁴³ Controversially the ICO, which was under pressure from the Conservative policing minister at the time Chris Philp,⁴⁴ took advisory action (which upon our filing an FOIA request was heavily redacted) but did not take any further regulatory action.

Despite this decision, members of the public who have been wrongly placed on watchlists or misidentified by retail LFR software frequently contact us. In May 2024, Big Brother Watch supported a teenager who was stopped in a Home Bargains store, wrongly accused of being a thief, subjected to a bag search, told to leave the store, and banned from other stores across the country.⁴⁵ In subsequent correspondence between Facewatch and the claimant, Facewatch admitted that its technology and an employed human "super-recogniser" were

⁴² Facewatch website, <https://www.facewatch.co.uk/>.

⁴³ Letter from Information Commissioner's Office to Facewatch following investigation, 28 March 2023, <https://bigbrotherwatch.org.uk/wp-content/uploads/2023/06/Closure-letter-redacted.pdf>.

⁴⁴ The Guardian, Revealed: Home Office secretly lobbied for facial recognition 'spy' company, 2 September 2023, <https://www.theguardian.com/technology/2023/sep/02/home-office-accused-of-secret-lobbying-for-facial-recognition-spy-company>.

⁴⁵ BBC, 'I was misidentified as shoplifter by facial recognition tech', 26 May 2024, <https://www.bbc.co.uk/news/technology-69055945>.

responsible for the misidentification. Despite Facewatch's reassurances following the ICO's investigation that they would focus on "repeat offenders or individuals committing significant offences,"⁴⁶ Big Brother Watch assisted a 62-year-old woman who was put on a Home Bargains watchlist and blacklisted from her local stores after being wrongly accused of stealing paracetamol worth 39 pence.⁴⁷ Other members of the public have been wrongly added to watchlists after being falsely accused of stealing a bottle of wine,⁴⁸ toilet roll⁴⁹ and after being mistaken for another "bald-headed, bearded customer."⁵⁰ We are concerned that people who have contacted Big Brother Watch and publicly shared their stories in national media only represent the tip of the iceberg of those misidentified by LFR.

The European Data Protection Board has stated that the use of LFR by private entities for their own purposes, including security, requires explicit consent from all data subjects in most cases.⁵¹ This means that retailers using LFR would have to set up a separate entrance for customers who want to opt-out of biometric surveillance and cannot make access to their services conditional on accepting biometric processing. European data regulators have also shown more willingness to enforce data protection law by sanctioning companies who do not comply. Following similar complaints to Big Brother Watch's complaint to the ICO about Facewatch, the data protection authority in the Netherlands ruled that the use of LFR in retail stores was "disproportionate"⁵² and the Spanish regulator fined a supermarket 2,520,000 EUR for its unlawful use of the software.⁵³ The Australian data protection regulator also determined that the retailer, Bunnings Group Limited breached the privacy rights of hundreds of thousands of Australians by collecting their sensitive personal information via their facial recognition software system.⁵⁴

⁴⁶ Information Commissioner's Office, Blog: Balancing people's privacy rights with the need to prevent crime, 31 March 2023, <https://ico.org.uk/about-the-ico/media-centre/blog-balancing-people-s-privacy-rights-with-the-need-to-prevent-crime/>.

⁴⁷ The Guardian, 'Shopper put on facial ID watchlist after dispute over 39p of paracetamol at Home Bargains,' 6 June 2025, <https://www.theguardian.com/uk-news/2025/jun/06/shopper-facewatch-watchlist-39p-paracetamol-london>.

⁴⁸ Daily Mail, 'Innocent shoppers accused of wrongdoing by AI system: Warnings over Facewatch in stores like Sainsbury's, Budgens and B&M,' 5 January 2026, <https://www.dailymail.co.uk/news/article-15434955/Innocent-shoppers-accused-wrongdoing-AI-Facewatch-Sainsburys-Budgens-catch-crooks-creators-say-human-error-blameless-customers-getting-wrongly-accused.html>.

⁴⁹ BBC News, 'Woman mistaken for thief after shop face scan alert,' 14 June 2025, <https://www.bbc.co.uk/news/articles/cdr510p7kymo>.

⁵⁰ BBC News, 'Human error' blamed for facial recognition alert mix-up,' 18 August 2025, <https://www.bbc.co.uk/news/articles/c0ql4k35n0wo>.

⁵¹ European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices, Version 2.0, 29 January 2020, para 77, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf.

⁵² Dutch DPA issues Formal Warning to a Supermarket for its use of Facial Recognition Technology, European Data Protection Board, 26th January 2021, accessed 5th December 2024, https://www.edpb.europa.eu/news/national-news/2021/dutch-dpa-issues-formal-warning-supermarket-its-use-facial-recognition_en.

⁵³ Spanish DPA Fines Supermarket Chain 2,520,000 EUR for Unlawful Use of Facial Recognition System, Hunton Andrew Kirths, 30th July 2021, accessed 5th December 2024, <https://www.huntonak.com/privacy-and-information-security-law/spanish-dpa-fines-supermarket-chain-2520000-eur-for-unlawful-use-of-facial-recognition-system>.

⁵⁴ Facial recognition technology in retail settings: after the Bunnings decision, office of the Australian Information Commissioner, 19 November 2024, accessed 5th December 2024,

The EU AI Act facial recognition provisions do not specifically address the private sector as it is considered to already be covered under GDPR.⁵⁵ The legislation explains that “the use of remote biometric identification for purposes other than law enforcement has already been subject to prohibition decisions by national data protection authorities.”⁵⁶ However, given the ICO’s failure to adequately protect data protection rights in the UK, the new legislative framework represents an opportunity to explicitly restrict the use of mass private sector LFR in publicly accessible places, as well as FRT and similar technologies by non-law enforcement agencies. Indeed, the European Digital Rights Network (EDRi) argued that the EU AI Act would have also been strengthened by explicitly prohibiting private uses of FRT for law enforcement purposes⁵⁷

2.2 Non-law enforcement organisations using FRT for non-law enforcement purposes

Non-law enforcement organisations are also using FRT for non-law enforcement purposes. Given the intrusive nature of this technology, the new legislative framework should explicitly ban such uses.

In November 2022, Big Brother Watch issued an ICO complaint against online facial recognition ‘search engine’ PimEyes, arguing that the company is unlawfully processing the biometric data of millions of UK citizens. PimEyes allows anyone to upload an input image, which is compared against an index of billions of photos on the internet without any safeguards. In December 2022, the German data protection agency initiated fine proceedings against PimEyes, citing the “massive threat to the rights and freedoms of citizens,” as well as “apparent lack of data protection compliance and the significant deficiencies in PimEyes’ technical and organisational measures.”⁵⁸ However, the ICO declined to investigate PimEyes, citing the ongoing German investigation.

The ICO’s resources are outstripped by the magnitude of the private FRT industry, let alone the rest of the big data market. In the context of the ICO’s limited regulatory capacity, the new legislative framework should adopt the approach of the EU AI Act in expressly prohibiting the “use of AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage.”⁵⁹ The Act explains that FRT scraping practices, like those of PimEyes, “add[s] to the feeling of mass surveillance and can lead to gross violations of fundamental rights, including the right to privacy.”⁶⁰

Members of the public who are concerned about having to submit to LFR checks in order to access places of employment, sporting events and gyms frequently

<https://www.oaic.gov.au/news/blog/facial-recognition-technology-in-retail-settings-after-the-bunnings-decision>.

⁵⁵ Recital 39.

⁵⁶ Recital 39 of the EU AI Act.

⁵⁷ EDRi, ‘Remote biometric identification: a technical & legal guide,’ 23 January 2023, <https://edri.org/our-work/remote-biometric-identification-a-technical-legal-guide/>.

⁵⁸ Baden-Wuerttemberg Press Release, ‘PimEyes: LfDI opens fine procedure,’ 21 December 2022, <https://www.baden-wuerttemberg.datenschutz.de/pimeyes-ldi-eroeffnet-bussgeldverfahren/>.

⁵⁹ Article 5(1)(e) of the EU AI Act.

⁶⁰ Recital 43 of the EU AI Act.

contact Big Brother Watch.⁶¹ Last year, The Football Supporters Association passed a motion opposing the introduction of FRT at turnstiles or inside stadia based on concerns about the potential for monitoring and tracking in future.⁶² The ICO makes clear that there should be alternatives in place if the lawful basis for processing is consent.⁶³ However, in the absence of regulatory enforcement capacity, the new legislative framework is an opportunity to make clear that unavoidable biometric scans are not an appropriate or necessary obligation.

Given the expansion of FRT functions in every day commercially available technology, such as Amazon's development of a facial detection feature in Ring doorbells⁶⁴ and demographic scanning digital billboards,⁶⁵ which subject non-consenting members of the public to biometric identity checks, the new legal framework should take a broadly prohibitive approach with carve outs for only the most necessary and proportionate uses of FRT.

3. When should law enforcement organisations be allowed to use these technologies? [Q6-9, 12-13]

3.1 Interference with fundamental rights

The capacity of police forces to identify individuals using facial images obtained from photographs or video poses a serious threat to anonymity in public spaces. It is relevant that this ability to track and monitor individuals across time and space uses facial features as biometric identifiers. Our faces are deeply personal, difficult to conceal, and impossible to change absent significant cost or injury. In order to comply with human rights law the processing of sensitive biometric personal data must be subject to strict regulation.

3.1.1 Privacy rights

It is not disputed that FRT infringes privacy rights. In the case of *Bridges v South Wales Police*, the Divisional Court held that automated FRT "enables the extraction of unique information about an individual allowing his or her identification with precision in a wide range of circumstances, and that AFR [Automated Facial Recognition]-derived biometric data is information of an intrinsically private character."⁶⁶ The use of all forms of FRT therefore engages the right to privacy under Article 8 of the Human Rights Act 1998. Public authorities may only infringe upon this fundamental right where they have a

⁶¹ Big

⁶² Football Supporters' Association, 'Facial recognition turnstiles: Why supporters should be concerned,' 27 June 2025, <https://thefsa.org.uk/news/facial-recognition-turnstiles-why-supporters-should-be-concerned/>.

⁶³ Information Commissioner's Office, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-process-biometric-data-lawfully/>.

⁶⁴ The Times, Police and Amazon build 'surveillance state' with free all-seeing doorbells, 8 September 2019, <https://www.thetimes.com/business/technology/article/police-and-amazon-build-surveillance-state-with-free-all-seeing-doorbells-dwdt3t6q0>.

⁶⁵ The Guardian, UK campaigners condemn 'creepy' digital billboards that can track viewers' responses, 9 December 2025, <https://www.theguardian.com/world/2025/dec/09/uk-campaigners-condemn-digital-billboards-track-viewers>.

⁶⁶ [2019] EWHC 2341 (Admin) [57]

legitimate aim and the interference is in accordance with the law, necessary, and proportionate.

3.1.2 Free expression, assembly and association

Law enforcement use of FRT also interferes with free expression and free assembly rights under Articles 10 and 11 of the HRA 1998 when used in the context of protests and public demonstrations. Freedom of assembly and association have traditionally relied on a degree of anonymity to afford participants protection against being singled out or identified. There is a distinct risk that if FRT is used to identify protestors it will create a chilling effect that could cause individuals to modify their behaviour. If attendees know that they can be identified in real-time or that police forces can use RFR on images or videos captured in public spaces they may feel unable to express their beliefs in the same way or at all, infringing on their free expression rights. Indeed, this was the argument Big Brother Watch Director Silkie Carlo and campaigner Ed Bridges made in their respective legal challenges against the police use of LFR.

The “chilling effect” of surveillance technology has also been recognised by UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, the European Court of Human Rights,⁶⁷ and rights groups around the world. The UN High Commissioner for Human Rights recognised the unprecedented threat posed by FRT in a 2020 report, which stated:

“The rise of facial recognition technology has led to a paradigm shift in comparison with practices of audiovisual recordings, as it dramatically increases the capacity to identify all or many participants in an assembly in an automated fashion (...)

The negative effects of the use of facial recognition technology on the right of peaceful assembly can be far-reaching (...) Many people feel discouraged from demonstrating in public places and freely expressing their views when they fear that they could be identified and suffer negative consequences.”⁶⁸

These fears are especially pertinent giving existing policing powers to capture and retain footage from protests for decades.⁶⁹

There is precedent for UK police forces using LFR to target protestors. For example, South Wales, Northamptonshire and the Metropolitan Police have used LFR at an anti-arms’ fair demonstration in Cardiff,⁷⁰ against climate activists

⁶⁷ *Glukhin v Russia* (Application no. 11519/20)

⁶⁸ Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests: Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General – UN Human Rights Council, 24th June 2020, A/HRC/44/24: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/154/35/PDF/G2015435.pdf?OpenElement>

⁶⁹ Statewatch, ‘UK: Police footage of protests can be held for decades,’ 2 October 2025, <https://www.statewatch.org/news/2025/october/uk-police-footage-of-protests-can-be-held-for-decades/>.

⁷⁰ BBC News, Facial recognition use by South Wales Police ruled unlawful, 11 August 2020, <https://www.bbc.co.uk/news/uk-wales-53734716>.

during the Formula One British Grand Prix at Silverstone,⁷¹ and at other high-profile events attracting peaceful demonstrations such as the Coronation of King Charles III.⁷² In Europe, the Hungarian government passed legislation allowing the police to use LFR to identify participants at LGBTQIA+ public events in breach of Article 5 of the EU AI Act.⁷³ In Hong Kong, protestors resorted to using masks and umbrellas to conceal their faces.⁷⁴

The rights group EDRI argues that both LFR and RFR have a significant impact on human rights, as they may infringe on individuals' willingness to seek healthcare, legal advice, visit LGBTQIA+ venues, participate in democratic processes like voting and political activism and expressing gender, sexual, or religious identity.⁷⁵ Given the implications for fundamental rights, the threshold for using FRT must be sufficiently prohibitive, particularly in relation to public assemblies and protests.

3.2 Necessity and proportionality

3.2.1 Seriousness of harm

In recognition of the intrusive nature of FRT, the legislative framework should strictly limit police use. It would be disproportionate for police forces to use FRT to target low-level crime. If police do use FRT, they should only do so to investigate serious crime, which must be strictly defined to set a meaningful threshold on its use. The definition of serious crime used by the Metropolitan Police Service (MPS), of any "recordable offence for which an adult is capable of being sentenced to one year or more in prison,"⁷⁶ is so broad as to render it a redundant safeguard in practice. Further, the new legislative framework should make it clear that a deployment authorised on the basis of a serious crime cannot be used to justify adding related people wanted for lower-level offences to the watchlist.

For police use of LFR, the new legislative framework should prohibit this technology entirely or adopt the EU AI Act as the floor for its deployment. In the EU, member states can only use LFR to locate or identify people suspected of committing a criminal offence where strictly necessary for investigating crime or prosecuting a criminal penalty for offences listed under Annex II and punishable by a custodial sentence or a detention order for a maximum period of at least four

⁷¹ BBC News, 'F1 British Grand Prix: Facial recognition at Silverstone being used,' 6 July 2023, <https://www.bbc.co.uk/news/uk-england-northamptonshire-66120010>.

⁷² The Guardian, Police accused over use of facial recognition at King Charles's coronation, 3 May 2023, <https://www.theguardian.com/uk-news/2023/may/03/metropolitan-police-live-facial-recognition-in-crowds-at-king-charles-coronation>.

⁷³ The Civil Liberties Union for Europe (Liberties), Facial Recognition to Target Pride in Hungary: Civil Society Orgs Call On The EU to Commit to Rights and Rule of Law, 24 June 2025, <https://www.liberties.eu/en/stories/hungary-facial-recognition-pride/45453>.

⁷⁴ The Guardian, This article is more than 3 years old
The big picture: umbrellas shielding democracy in Hong Kong, 11 December 2022, <https://www.theguardian.com/artanddesign/2022/dec/11/the-big-picture-umbrellas-shielding-democracy-in-hong-kong>.

⁷⁵ EDRI, 'Remote biometric identification: a technical & legal guide,' 23 January 2023, <https://edri.org/our-work/remote-biometric-identification-a-technical-legal-guide/>.

⁷⁶ Metropolitan Police Service, Overt LFR policy document, 11 September 2025, p24, <https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/policy-documents/lfr-policy-document2.pdf>.

years.⁷⁷ It is important that the new legislative framework sets out the specific serious criminal offences for which it regards LFR to be necessary and proportionate, otherwise it would become very easy for future governments to dramatically expand the use of facial recognition without democratic oversight, merely by increasing sentences.

For RFR and LFR, a biometric search should only be undertaken when the individual in the image is suspected of carrying out a qualifying offence, namely sexual, violent, terrorism, and burglary offences as defined by Section 65A of the Police and Criminal Evidence Act 1984. Qualifying offences are also used as a threshold in policies governing police retention of fingerprint and DNA data, which make them an appropriate threshold for facial biometric data. Victims, witnesses, and associates should not be subject to LFR or RFR searches. Restricting LFR and RFR searches to qualifying offences allows police reasonable use of the technology to identify criminals who pose a serious risk to the public while preventing the mass, indiscriminate use of the technology for any policing need. With regard to RFR, this threshold should apply to both one-to-many searches (a search of a probe image against an image reference library) and one-to-one searches. In addition to setting out specific offences for which LFR and RFR may be justifiable, it may also be appropriate to include a provision restricting its use to cases where the sought person could reasonably be expected to be sentenced to imprisonment for a term four years or more to ensure it is aligned with the EU AI Act and can only be used where proportionate.

Qualifying offences should act as a baseline requirement for the use of RFR such that it cannot be deployed outside investigations into these narrowly defined offences. However, this baseline only represents a starting point and RFR need not be used in every instance where police are investigating a qualifying offence. Where more proportionate means of identifying a suspect are available they should be pursued in the first instance. Considerations such as the characteristics of the victim and urgency arising from a threat to life or safeguarding concerns should be assessed at that stage of the test.

3.2.2 Less intrusive means

There is currently no requirement for the police to pursue other investigative leads before adding individuals to a watchlist and justifying a LFR deployment. As a result, sought persons may be added to police watchlists without the police having done taken any efforts to find the individual, such as visiting their home address or making inquiries, which would be far less intrusive than taking biometric scans of millions of law-abiding people. The new legislative framework must include a requirement for all other options to be exhausted before a sought person is added to a watchlist.

In addition to the seriousness of the harm the interference is seeking to prevent or detect, the urgency of the harm is also relevant. This is because there may be

⁷⁷ Annex II identifies the following offences: terrorism, trafficking in human beings, sexual exploitation of children, and child pornography, illicit trafficking in narcotic drugs or psychotropic substances, illicit trafficking in weapons, munitions or explosives, murder, grievous bodily injury, illicit trade in human organs or tissue, illicit trafficking in nuclear or radioactive materials, kidnapping, illegal restraint or hostage-taking, crimes within the jurisdiction of the International Criminal Court, unlawful seizure of aircraft or ships, rape, environmental crime, organised or armed robbery, sabotage, participation in a criminal organisation involved in one or more of the offences listed above.

more proportionate measures that can be taken to investigate the offence and attempt to identify the individual using less intrusive means. Failure to do so could result in police relying on FRT as the default option without considering its necessity in the specific case.

3.2.3 Proportion of publicly-accessible spaces covered

Under current police force policies, the location for an LFR deployment can be chosen on the basis that one person on the watchlist is likely to be at the relevant location. In practice, this means that the police can target crowded and publicly-accessible areas simply because they know vast numbers of people will be there whom they can search. Police forces should only be able to deploy LFR where there is a connection, underpinned by specific intelligence, between the individual being sought and the location.

The cumulative effect of LFR is also a relevant consideration. Whilst members of the public may be able to avoid certain geographically limited areas where they know LFR is in use (albeit, the extent to which this is possible is disputed), this alternative becomes impossible where it is being deployed constantly across vast swathes of the country. As a result, the areas where people are able to participate in public life becomes increasingly diminished.

3.2.4 Probe images

The origin of the probe images is a relevant factor when considering how law enforcement use of FRT interferes with fundamental rights. Photos and videos obtained lawfully during policing operations, police body cam footage taken in a lawful and proportionate way, and lawful custody images are appropriate for RFR, provided the other strict requirements of proportionality and necessity are met. However, hundreds of thousands of police-originated photos in the Police National Database are of innocent people who are unaware that their unlawfully held images are being processed in RFR searches. Despite a 2012 High Court ruling which held that indefinite retention of innocent people's custody images is unlawful, police officers have put the onus on individuals to request deletion, rather than manually reviewing their databases.⁷⁸ As a result of this failure to remove unlawfully-held images, innocent people face a growing risk of being wrongly identified by RFR searches with potentially devastating consequences.

Police forces also use non-police originated images such as CCTV footage, social media photos and videos and smart doorbell or dashcam footage, for FRT checks. These non-police originated probe images attract a greater expectation of privacy than compliant police originated probe images, which are preferable. Police should not be permitted to use external tools, such as PimEyes, to conduct RFR searches. In 2024, Liberty Investigates revealed that the Met Police accessed the FRT search engine on 2,337 occasions over a three-month period.⁷⁹ There were no restrictions on the officers who were able to use the engine, nor any safeguards around the probe images used or a requirement for making official records of the searches. Images from non-police or non-compliant

⁷⁸ *RMC and FJ v Commissioner of Police of the Metropolis* [2012] EWHC 1681 (Admin).

⁷⁹ Liberty Investigates, Met police computers access 'dangerous' facial recognition search engine, 10 May 2024, <https://libertyinvestigates.org.uk/articles/met-police-computers-access-dangerous-facial-recognition-search-engine/>.

sources should be used only when other options have been exhausted and law enforcement agencies should be prohibited from using external third-party tools.

3.2.5 Databases being searched

The databases which law enforcement agencies can use to conduct FRT searches should also be restricted to limit infringements on human rights. Earlier uses of RFR relied on pre-existing databases of police-originated images, such as the Police National Database or individual forces' own custody image databases. However, Liberty Investigates revealed that police forces have been using the passport database covertly since at least 2019 to conduct hundreds of facial recognition searches of 46 million British passport holders.⁸⁰

The Government is currently seeking to formalise the appropriation of near population-wide databases for the purposes of RFR under the Crime and Policing Bill being debated in parliament. Clause 95 of the Crime and Policing Bill (in House of Lords Committee Stage at time of writing) would allow the Secretary of State to create regulations which grant police digital access to DVLA records for "purposes relating to policing or law enforcement." Subverting near population-wide image databases, such as the DVLA, passport or proposed Digital ID database, to run FRT searches would affect the majority of adults who have done nothing to arouse suspicion and would be a highly disproportionate interference with the right to privacy.

Biometric sampling of population-wide databases is also likely to be unlawful. In the case of *S and Marper v the UK*, the European Court of Human Rights held that the blanket and indiscriminate retention of biometric and DNA data of individuals not convicted of offences failed to strike a fair balance between the competing public and private interests.⁸¹ The dangers of linking expansive population-wide databases to facial recognition systems can be seen in the United States, where Customs Enforcement Officers are using OIFR to investigate the citizenship status of members of the public, including US citizens, resulting in a serious chilling effect and discriminatory effects on communities of colour.⁸² In order to ensure that the data collection and processing involved in conducting an RFR search is proportionate, police RFR searches should be restricted to databases of known offenders.

4. Authorisation and oversight [Q10-11, 14-17]

4.1 Authorisation

The EU AI Act requires that each use of LFR in publicly accessible spaces for law enforcement purposes occurs pursuant to "prior authorisation granted by a judicial authority or an independent administrative authority whose decision is binding."⁸³ In circumstances of genuine urgency police can deploy LFR without prior authorisation, provided authorisation is sought "without undue delay, at the

⁸⁰ Liberty Investigates, 'Police secretly conducting facial recognition searches of passport database', 8 January 2024, <https://libertyinvestigates.org.uk/articles/police-secretly-conducting-facial-recognition-searches-of-passport-database/>.

⁸¹ *S and Marper v United Kingdom* (Applications nos. 30562/04 and 30566/04)

⁸² <https://www.npr.org/2025/11/08/nx-s1-NPR5585691/ice-facial-recognition-immigration-tracking-spyware>

⁸³ Article 5(3) of the EU AI Act

latest within 24 hours.”⁸⁴ The new legislative framework should adopt the same restrictions as a minimum to ensure the use of LFR is subject to strict oversight, accountability, and transparency. The question of what constitutes urgency should be well-defined to avoid overuse of this power.

Where RFR is conducted using non-police-originated probe images or databases, it should be authorised by a body independent of law enforcement organisations. This reflects the authorisation process of Investigatory Powers Commissioner’s Office (IPCO), which makes decisions on requests for communications data from law enforcement and certain other public authorities under the Investigatory Powers Act 2016 (IPA).

4.2 Oversight body

We support the proposal for a single independent oversight body which incorporates and expands the current role of the Biometrics and Surveillance Camera Commissioner. As the legislative framework should be restrictive by default rather than permissive, the regulator’s role would be infrequently concerned with use cases and would be focused on oversight. The scope of the oversight body should extend to all uses of FRT, not just cases where it is used for policing purposes.

The oversight body should be empowered to allow for ongoing review of how the powers are being applied, investigate potentially unlawful uses of FRT and set testing standards to assure scientific validity of algorithms. It must have sufficient powers to compel information and undertake enforcement action to prevent it from becoming a toothless regulator. The oversight body has a role to play in investigating instances where a technology has been misused, hacked, or accessed without authorisation; requesting information; issuing compliance notices; seeking injunctions making public declarations; receiving complaints; publishing an annual report; and deciding which new technologies the police and private sector can use.

4.3 Algorithmic accountability – bias and discrimination

LFR suffers with well-documented issues relating to accuracy and race and gender bias. Big Brother Watch has witnessed the MPS misidentify children in school uniforms using LFR and then subject them to lengthy, humiliating, and aggressive police stops in which they were required to prove their identity and provide fingerprints. In two such cases, the children were young black boys and both children were scared and distressed. One of these stops was also witnessed by the MPS’ Independent Reviewer, Professor Peter Fussey, who remarked on how “distressed and clearly intimidated” the child was.

In April 2023, the MPS and South Wales Police commissioned a report into the accuracy of their LFR system from the National Physical Laboratory (NPL). The Home Office and all ten police forces deploying LFR have relied on the NPL report to suggest that there is no statistically significant difference between the technology’s performance across different demographics. This is despite the fact that the study tested only one algorithm, the NEC’s NeoFace M40 algorithm, and not all police forces use the same LFR software. The performance of various

⁸⁴ Ibid.

algorithms varies significantly. We have serious concerns about the limitations of this report and how its findings have been presented by the police.

The report found that the police's LFR software is in fact less accurate for women and people of colour, although this bias reduces when a higher accuracy threshold is set to limit match alerts, specifically above the 0.60 similarity score threshold. However, police forces have operated the technology at lower settings in the past and there are no safeguards to prevent them from doing so in the future. At the 0.60 threshold 13 Black and Asian individuals were still falsely flagged, whilst no white individuals were misidentified. There is a greater margin of error when LFR technology is deployed in real-life settings compared to laboratory test conditions. As the number of faces scanned grows even a small probability means that hundreds, if not thousands, of individuals could be wrongly flagged and forced to prove that they are not who the technology says they are.

Given that misidentifications are more likely to affect certain groups, they could exacerbate the existing inequalities in policing. We have found this concern borne out during our observations of deployments. In February 2024, Shaun Thompson, a black anti-knife crime community worker, was misidentified by the Metropolitan Police's facial recognition system, which was deployed near London Bridge. He was held up by the police for almost 30 minutes as they made him prove he was not the individual on the watchlist by showing multiple ID documents. Police also demanded scans of his fingerprints and threatened him with arrest when he declined. Mr Thompson is now bringing a legal challenge against the MPS' use of facial recognition, arguing that it constitutes an unlawful interference with his Article 8 right to privacy. The MPS maintains that its use of LFR is lawful.

The related issues of who is included on police watchlists and where deployments take place are also cause for concern. The MPS has deployed LFR in Croydon more than any other borough since trials began in 2016. Singling out black and brown communities for increased biometric surveillance risks reinforcing existing biases in policing, or as Shaun Thompson put it, acts as "stop and search on steroids".

A new oversight body would be well-placed to set specific rules for law enforcement organisations to follow to guard against bias and discrimination when using technologies such as FRT.