BIG BROTHER WATCH

PRIVATE SECTOR USE OF LIVE FACIAL RECOGNITION: Q&A BRIEFING

Q1. How does live facial recognition (LFR) work?

Live facial recognition (LFR) matches faces on live surveillance camera footage against a watchlist in real time. Companies add individuals who they want to exclude from a store to a tailored watchlist, which generally comprises of images taken from the customers' previous visits to a store. Facial recognition software companies also offer 'National Watchlists' comprised of uploads of images and reports of incidents of crime and disorder from its customers across the UK.

A camera placed at the entrance of a store will then capture a live video feed, from which the LFR software will detect human faces, extract the facial features and convert them into a biometric template to be compared against those held on the watchlist. The software generates a numerical similarity score to indicate how similar a captured facial image is to any face on the watchlist. Any matches above this pre-set threshold are flagged to shop staff, who then deal with the individual in line with the retailers' policy.

Q2. What are the risks of this technology?

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. In recent years, parliamentarians across parties in Westminster,[1] members of the Senedd,[2] rights and equalities groups and technology experts across the globe have called for a stop to the use of this technology.[3]

There is a particularly chilling, and entirely foreseeable, risk that the UK's vast CCTV camera network could be updated with LFR-enabled cameras. Existing facial recognition

[1] MPs and peers call for 'immediate stop' to live facial recognition surveillance – Jamie Grierson, the Guardian, 6 October 2023: https://www.theguardian.com/technology/2023/oct/06/mps-and-peers-call-for-immediate-stop-to-live-facial-recognition-surveillance

[2] Concerns raised about 'intrusive' use of live facial recognition technology - Nation Cymru, December 2023: https://nation.cymru/news/concerns-raised-about-intrusive-use-of-live-facial-recognition-technology/

[3] Over 180 Rights Groups and Tech Experts Call for UK and Worldwide Halt to Facial Recognition Surveillance – Josiah Mortimer, Byline Times, 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/

software can be added to almost any brand of CCTV camera, which means a huge network of privatised facial recognition could be rolled out across the UK. Such a system of surveillance would produce a level of biometric intrusion that has never before been contemplated in a democracy and is more commonly associated with countries that have authoritarian regimes. The prevalence of facial recognition as a feature of CCTV cameras available on the wider market risks normalising the technology regardless of the threat it poses to rights and privacy.

The software is also open to abuse. Despite some protections being provided by the Data Protection Act 2018 and UK GDPR, we have seen that facial recognition software companies have been able to operate with very little scrutiny or regulatory oversight. Given this reality, there is potential for facial recognition software to be used as a tool for socio-economic discrimination. Before it was updated, the facial recognition software company Facewatch's policy, permitted its customers to include individuals on the watchlist for anti-social behaviour, which includes begging, street drinking and vagrancy.[4] Clearly, these are not criminal offences, but their inclusion suggests that companies seek to use this software not only to prevent crime but to eliminate so-called "undesirables" from the public sphere. Indeed, in a (now private) video published by Facewatch, which has since been deleted, showed its product development manager discussing the aim of discouraging "undesirables" and people who are "generally causing trouble" from entering a store.[5] The asymmetry of power and absence of regulation sets a dangerous precedent, whereby those operating the software can significantly impact the rights of an individual to access services.

Q3. Does LFR have a legal basis?

Private use of live facial recognition is regulated by the Data Protection Act 2018 and UK GDPR, however the Information Commissioner's Office ('ICO') has been slow to intervene over concerns about the lawfulness of the private use of LFR. In July 2022, Big Brother Watch filed a legal complaint to the ICO, in relation to the use of Facewatch's LFR software in Southern Co-op stores. Following an investigation, the ICO concluded in March 2023 that Facewatch's data processing had breached data protection laws on a number of principles, including lawfulness, fairness and transparency, purpose limitation, storage limitation, lawfulness of processing, processing of special categories of data, processing of personal data in relation to criminal convictions and offences and the rights of children. Following private correspondence between the ICO and Facewatch, the company was forced to overhaul their data processing practices.

However, we maintain that the company's data processing still does not meet data protection and human rights standards. We have been contacted by numerous individuals

[4] Facewatch User Guide, accessed 22nd March 2023: https://www.facewatch.co.uk/wp-content/uploads/2020/04/User-Guide-V1.1-web.pdf

[5] George's Tech Tips – Vlog #1 Introduction, Facewatch, YouTube, 11th May 2020, accessed 23rd May 2023, https://www.youtube.com/watch?v=jic-114_bil

who have been wrongly stopped and misidentified by facial recognition, including the following cases:

> A teenage girl, Sara, was misidentified by live facial recognition in a Home Bargains store, accused of being a shoplifter, subjected to a bag search, removed from the store and barred from other shops using the software.[6]
>
> A 64-year-old woman was falsely accused of stealing less than £1’s worth of paracetamol by Home Bargains and wrongly added to a facial recognition watchlist.[7]
>
> Danielle Horan was wrongly placed on Facewatch’s facial recognition watchlist, was labelled a thief and had her biometric data shared between shops in her area using the technology, alongside the erroneous accusation. She was twice accused of being a shoplifter and removed from stores, despite being innocent.[8]

Other forms of biometric processing, such as fingerprinting and DNA testing, are subject to strict controls and oversight deriving from specific legislation. From a rule of law perspective, it is imperative that the law is clear, intelligible and predictable and protects fundamental human rights.[9] It remains that the words ‘facial recognition’ are not contained in a single Act of Parliament.

Q4. How accurate is LFR, and does it have a race bias?

Live facial recognition suffers with well-documented issues relating to accuracy and race and gender bias. Whilst private facial recognition companies may give assurances about the accuracy and efficacy of their products, they are, in the absence of any regulatory scrutiny, in affect able to mark their own homework. Given that misidentifications are more likely to impact certain groups, this could lead to private companies unlawfully discriminating against individuals who are flagged by LFR.[10]

We have been contacted by dozens of individuals who have been wrongfully stopped and misidentified in stores where LFR technology is being used. Those affected report having anxiety about visiting other stores who use the technology and feeling embarrassed and humiliated about being so publicly stopped for no apparent reason. It is especially difficult for those on watchlists to find out what they are accused of. Frequently, individuals have

[6] Landmark legal challenges launched against facial recognition after police and retailer misidentifications – Big Brother Watch press release: https://bigbrotherwatch.org.uk/press-releases/landmark-legal-challenges-launched-against-facial-recognition-after-police-and-retailer-misidentifications/

[7] Shopper put on facial ID watchlist after dispute over 39p of paracetamol at Home Bargains – Daniel Boffery, the Guardian, 6 June 2025: https://www.theguardian.com/uk-news/2025/jun/06/shopper-facewatch-watchlist-39p-paracetamol-london

[8] Woman mistaken for thief after shop face scan alert – BBC News, 14 June 2025: https://www.bbc.co.uk/news/articles/cdr510p7kymo

[9] The Rule of Law - Lord Bingham, Penguin Books, 2011

[10] See for example, The Baroness Casey Review: An independent review into the standards of behaviour and internal culture of the Metropolitan Police Service, March 2023, https://www.met.police.uk/SysSiteAssets/media/downloads/met/about-us/baroness-casey-review/update-march-2023/baroness-casey-review-march-2023a.pdf

no idea why they may have been included and have to go to great lengths, including by submitting even more personal data – such as their ID, name and date of birth, to LFR software companies in order to get answers. We have assisted some of these individuals to submit subject access requests and initiate legal action. This produces a system of unaccountable private policing, within which people are accused of quasi-criminal offences without any recourse to challenging the claims.

Q5. Is LFR is necessary to catch shoplifters?

In the retail context, LFR is often touted as a solution to combat shoplifting and anti-social behaviour. Following the ICO's investigation of Facewatch, the regulator held that in order to comply with data protection legislation and human rights law, retailers could only place individuals on a watchlist where they are serious or repeated offenders. The evidence we have collated demonstrates that, in practice, members of the public are placed on retailers watchlists for very trivial reasons, including for accusations of shoplifting valued at only £1.[11] Not only are LFR companies not complying with regulatory decisions, but also the technology is being used disproportionately as it is not targeted at the most harmful perpetrators.

In the Justice and Home Affairs Committee Inquiry on 'Tackling Shoplifting,' Paul Gerrard, Public Affairs and Board Secreteriat Director at The Co-op Group, gave oral evidence that the company has no plans to implement LFR because it "cannot see what intervention it would drive helpfully."[12] Gerrard highlighted the ethical implications of employing a mass surveillance tool in a shop, as well as the heightened risk of violence and abuse to retail employees who have to confront shoppers if the LFR system flags them. His evidence reflects our position that there is no place for this invasive software from both the perspective of shoppers and retail workers.

Q6. Is private use of LFR just the modernisation of traditional security systems?

There is also a significant divergence between the level of intrusion associated with traditional security systems versus facial recognition surveillance. LFR is an invasive form of biometric surveillance, which is linked to a deeply personal identifying feature (i.e., an individual's face) and is deployed in public settings, often without the consent or knowledge of the person being subjected to checks. Additionally, unlike "traditional" blacklists held by shops, which might comprise of photographs of known local offenders, LFR could flag an individual in a shop they have not previously visited, producing a far greater magnitude for surveillance.

[11] Shopper put on facial ID watchlist after dispute over 39p of paracetamol at Home Bargains – Daniel Boffery, the Guardian, 6 June 2025: https://www.theguardian.com/uk-news/2025/jun/06/shopper-facewatch-watchlist-39p-paracetamol-london

[12] Uncorrected oral evidence: Tackling shoplifting, Justice and Home Affairs Committee, 3 September 2024, https://committees.parliament.uk/oralevidence/14920/html/

The private use of live facial recognition creates a new zone of privatised policing. It emboldens staff members to make criminal allegations against shoppers, without an investigation or any set standard of proof, and ban them from other stores employing the software. Clearly, when errors are made, this has profound implications for the lives of those accused, with little recourse for challenging the accusations. The lack of oversight and safeguards means that vulnerable individuals, including young people and those with mental health issues, are particularly at risk of being included on watchlists and leaves the door open to discriminatory and unfair decisions with significant impacts.

Q7. How have other states regulated LFR?

It is noteworthy that LFR is most enthusiastically embraced by authoritarian regimes, like Russia and China, whilst other democratic countries have taken measures to restrict its use. Several US states and cities have implemented bans and restrictions on the use of LFR and the EU has implemented the AI Act, which prohibits the use of LFR for law enforcement purposes, except in the most serious and strictly defined cases with a requirement of judicial authorisation. Private use of LFR is considered prohibited but could be made explicit in national law. This is a far cry from the UK's unregulated approach and lack of oversight.

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"[13] and the Spanish regulator fined a supermarket 2,520,000 EUR for its unlawful use of the software.[14]

Q8. Does human oversight mean that LFR is safe to use?

When the LFR software flags a potential match on the watchlist, a security officer or member of staff will generally approach the individual and tell them to leave the store. Despite this human involvement, we understand that those operating LFR systems put significant trust in LFR software, even when it has clearly made a mistake.

There are two avenues of possible failure when an individual is wrongly flagged by LFR. Either an individual can be misidentified by a facial recognition system, or they are correctly identified, but have been wrongly placed on the facial recognition watchlist in the first place. Automation bias (trusting the outputs of automated systems even when they

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

[14] Spanish DPA Fines Supermarket Chain 2,520,000 EUR for Unlawful Use of Facial Recognition System, Hunton Andrew Kirths, 30 July 2021, accessed 5 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

have made mistakes) and aggressive marketing from facial recognition companies means that those operating the systems often do not believe that the software could be wrong, and trust the technology over the individual in question.

In May 2024, Big Brother Watch supported a teenager who was stopped in a Home Bargains, wrongly accused of being a thief, subjected to a bag search, told to leave the store and banned from other stores across the country. In subsequent correspondence with the claimant, Facewatch, the LFR software company in use, admitted that its technology and “super-recogniser” produced this serious error, and that Sara was mistaken for another person. In another case, Danielle Horan was wrongly flagged as a shoplifter, after she was erroneously placed on Facewatch’s system. Both Sara and Danielle explained they were innocent to staff members at the time, but evidently, having a human verify the outputs of LFR systems does not safeguard against misidentifications and mistakes.

Q9. Is it true that ‘if you have nothing to hide, you have nothing to fear’?

We all have something to fear from the rise of mass surveillance technology in the UK. Knowing that the companies could obtain a biometric scan of your face without requiring suspicion as you walk down the high-street has a potentially chilling effect on the behaviours many citizens are ordinarily willing to engage in – including lawful activities which are essential to democratic participation, such as attending peaceful demonstrations.

As several case studies demonstrate, the claim that individuals who have nothing to hide have nothing to fear is untrue: Sara was stopped in a Home Bargains, had her bag searched by security, told to leave and banned from other stores due to an error on the LFR system, Facewatch. and the human “super-recogniser”.[15] Placing the onus on individuals to prove their identity and prove their innocence puts us at all at risk of having to defend ourselves against false accusations in the event we are wrongly flagged.

Q10. Does LFR have the support of the public?

The Ada Lovelace Institute has conducted nuanced research on public opinion towards LFR, concluding that the public does not trust the private sector to use facial recognition technology ethically and is insufficiently informed about its commercial uses. The research also indicated that the public expects the government to place limits on the use of facial recognition technology and supports companies pausing sales of the technology in the intervening time.

[15] Landmark legal challenges launched against facial recognition after police and retailer misidentifications, Big Brother Watch, 24 May 2024: https://bigbrotherwatch.org.uk/press-releases/landmark-legal-challenges-launched-against-facial-recognition-after-police-and-retailer-misidentifications/

The technology has also received significant cross-party backlash and condemnation from civil society. In October 2023, 65 Parliamentarians and 32 rights and race equality groups in the UK called for an immediate stop to LFR for public surveillance.[16]

Q11. Which retailers are currently using this technology?

Southern Co-op was the first supermarket to invest in facial recognition technology. It faced significant backlash.[17] Frasers Group have also invested in the technology, leading to a cross-party letter from almost 50 parliamentarians urging the owner, Mike Ashley, to stop using the technology.[18] Home Bargains and B&M also use Facewatch's technology, the company which faced an investigation from the ICO, and was found to have breached data protection law on eight counts.[19] Big Brother Watch has received dozens of reports from members of the public who have been misidentified by Facewatch's technology.

Asda announced it would be trialling the use of live facial recognition in several of its stores in 2025, and received over 5,000 emails of complaint in response.[20] Iceland have also indicated they will start using Facewatch technology.[21]

For more information contact:
Madeleine Stone, Big Brother Watch
madeleine.stone@bigbrotherwatch.org.uk

[16] 65 parliamentarians call for "immediate stop" to live facial recognition surveillance, Big Brother Watch, 6th October 2023, https://bigbrotherwatch.org.uk/press-releases/65-parliamentarians-call-for-immediate-stop-to-live-facial-recognition-surveillance/

[17] Southern Co-operative's use of facial recognition on customers prompts legal complaint – Sky News, 27 July 2022: https://news.sky.com/story/co-ops-use-of-facial-recognition-on-customers-prompts-legal-complaint-12659309

[18] Regulatory 'lacuna' around facial recognition threatens rights – Kingsley Hayes, Computer Weekly, 8 June 2023: https://www.computerweekly.com/opinion/Regulatory-lacuna-around-facial-recognition-threatens-rights

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

[20] Asda deluged by complaints after rolling out controversial technology in Manchester stores – Levi Winchester and William Morgan, Manchester Evening News, 25 April 2025: https://www.manchestereveningnews.co.uk/news/cost-of-living/asda-deluged-complaints-after-rolling-31506310

[21] Iceland trials facial recognition tech to help tackle crime – Steve Farrell, the Grocer 24 June 2025: https://www.thegrocer.co.uk/news/iceland-trials-facial-recognition-tech-to-help-tackle-crime/705919.article