BIG BROTHER WATCH

Big Brother Watch submission to the Justice and Home Affairs Committee's Inquiry on 'Tackling Shoplifting' on live facial recognition in the retail setting

September 2024

About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaigning organisation, fighting for a free future. We're determined to reclaim our privacy and defend freedoms at this time of enormous technological change. We're a fiercely independent, non-partisan and non-profit group who work to roll back the surveillance state and protect rights in parliament, the media or the courts if we have to. We publish unique investigations and pursue powerful public campaigns. We work relentlessly to inform, amplify and empower the public voice so we can collectively reclaim our privacy, defend our civil liberties and protect freedoms for the future.

Contact

Silkie Carlo

Director

Direct line: 020 8075 8478
Email: silkie.carlo@bigbrotherwatch.org.uk

Written Submission

1. Big Brother Watch welcomes the opportunity to brief members of the Justice and Home Affairs Committee as part of their inquiry into 'Tackling Shoplifting' , following your recent evidence sessions of 21 May and 3 September, which featured discussions on facial recognition surveillance. Our submission focuses on the data protection, justice and human rights implications of using live facial recognition surveillance in retail settings, in order that members of the Committee are provided with balance when considering this area of policymaking.

2. Live facial recognition technology works by detecting the face of every person that walks within the view of the camera. The system creates a biometric scan of every viewable person's face; it compares those biometric scans to a database of images on a watchlist; and it flags individuals 'matched' by the system. When these systems are used by private retailers, individual shops, or networks of shops, must create 'watchlists' of unwanted individuals. There is no criminal threshold for being placed on a watchlist, and private facial recognition companies such as Facewatch do not receive information from or send information to the police – it is effectively a privatised policing system. This means individuals can be placed on a private facial recognition watchlist and blacklisted from their high street (and subscribing retailers across the region) at the discretion of a security guard, without any police report being made, let alone a fair trial, and without the individual even being informed of their being added to a watchlist. Innocent people are at serious risk of being wrongly flagged by the technology – indeed, Big Brother Watch has supported legal action for a number of people who have been either wrongly added to private watchlists or publicly ejected from stores, searched and humiliated following private facial recognition misidentifications, as documented by the BBC.[1]

3. Given the manner in which they operate, there is no way for these systems to only scan the faces of only those who are suspected of antisocial behaviour or having committed an offence. The technology processes the facial biometric data – information as sensitive as a fingerprint – of every person entering the store. This is the equivalent of performing an identity check on every single customer. Data protection and human rights laws set a high bar for the processing of such sensitive data in order to protect the privacy and security of everyone in the UK. Subjecting thousands of innocent people to biometric identity checks without justification is not only intrusive, but is also disproportionate to the aim of reducing shop theft and infringes upon the right to privacy.

4. In our view, it is highly likely that such mass, indiscriminate biometric processing by private companies for loss prevention is unlawful under GDPR. Indeed, in 2021 the Spanish Data Protection Authority issued a EUR 2,520,000 fine under GDPR to Mercadona, one of the leading supermarkets in Spain, for its use of facial recognition (AEPD, Spain – PS/00120/2021). It is notable that the use of of live facial recognition surveillance has been prohibited by regulators across Europe under the GDPR, the same data protection framework that applies in the

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

United Kingdom.[2] Meanwhile, at a state level, the EU AI Act, passed earlier this year, broadly prohibits the use of live facial recognition surveillance by authorities given the extraordinary risks it poses to individuals' rights and freedoms.[3]

5. The Committee should also be aware of the potential for bias and discrimination within the algorithms that power the surveillance software. Studies have shown that LFR is less accurate for people with darker skin[4] and these statistical conclusions are backed by real-life experience. Big Brother Watch is currently supporting a woman of colour who has taken legal action against Home Bargains and the facial company Facewatch, after she was misidentified by their technology, publicly accused of theft and told she was banned from all Home Bargains stores across the country as well as other major retailers who use Facewatch's technology.[5] In subsequent correspondence with the claimant, Facewatch admitted that its technology and "super-recogniser" flagged the wrong person and produced this serious error.

6. We have received numerous reports of members of the public being flagged on these systems, approached by shop staff and accused of criminal activity and we expect that the aforementioned high-profile case and legal action we supported is only the tip of the iceberg. Outsourcing policing functions to a private company means that those who are flagged by the system have no trial process and no route to appeal. In one individual's case we are supporting, neither the retailer nor Facewatch can provide any evidence of the alleged theft that provides the basis of their inclusion on a watchlist, and the individual strongly denies having ever stolen anything – yet the individual remains technologically blacklisted from major high street stores via live facial recognition and treated as guilty, and has no way of proving their innocence. This Kafkaesque situation is diametrically opposed to the long-standing principles of law and justice in the United Kingdom. The distress associated with being publicly misidentified and/or wrongly accused of a crime can also have wider ramifications for individuals' lives and livelihoods, particularly if they are accused in front of their families, friends or colleagues. Companies that use LFR technologies risk not only facing data protection challenges, but also run the risk of perpetuating unlawful discrimination.

7. No laws in the UK specifically authorise, regulate or even contain the words "facial recognition", and the use of this technology has never been debated by MPs. In recent years, parliamentarians across parties in Westminster[6] and rights and equalities groups and technology experts across the globe have called for a stop to the use of this technology.[7] The only detailed inquiry into the use of live

2 https://www.reuters.com/technology/italy-outlaws-facial-recognition-tech-except-fight-crime-2022-11-14/; https://www.huntonak.com/privacy-and-information-security-law/spanish-dpa-fines-supermarket-chain-2520000-eur-for-unlawful-use-of-facial-recognition-system

3 Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI – European Parliament, 9th December 2023: https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai

4 http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdfs

5 https://www.bbc.co.uk/news/technology-69055945

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

7 Over 180 Rights Groups and Tech Experts Call for UK and Worldwide Halt to Facial Recognition Surveillance – Josiah Mortimer, Byline Times, 27th September 2023:

facial recognition by a parliamentary committee called for a stop to its use.[8] In this context, the questions raised by the committee of whether LFR technology can be used for privatised "pre-emptive" policing are particularly concerning.

8. In July 2022, Big Brother Watch filed a legal complaint to the Information Commissioner's Office against the Southern Co-op and Facewatch over the supermarket's use of Facewatch's live facial recognition software in its stores. The Commissioner conducted an investigation, which concluded in March 2023 and found that Facewatch's policies had breached data protection law on eight grounds, including by failing to balance the legitimate interest of Facewatch and their subscribers against the rights and freedoms of individuals. Big Brother Watch's research indicates that some of the changes Facewatch was resultingly required to make have not been made.
9. Live facial recognition has a serious detrimental impact on individuals' protected rights to privacy and free expression, whilst also posing the risk of perpetuating discrimination and undermining the principles of justice. Within this context we urge the committee to refrain from in any way endorsing the use or expansion of live facial recognition surveillance in the retail sector, and at the very least to take further evidence on its legal and rights implications.

https://bylinetimes.com/2023/09/27/over-180-rights-groups-and-tech-experts-call-for-uk-and-worldwide-halt-to-facial-recognition-surveillance

8 The work of the Biometrics Commissioner and the Forensic Science Regulator: Nineteenth Report of Session
2017–19, Science and Technology Committee, 18th July 2019, HC 1970:
https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1970/197002.html