

FAO Layla Moran MP
Health and Social Care Committee,
House of Commons,
London, SW1A 0AA

30 July 2026

By email only

Dear Layla Moran MP,

I am writing on behalf of the civil liberties campaign group Big Brother Watch in relation to recent reports that live facial recognition (“LFR”) could be deployed in pharmacies across the UK.

Facewatch, the UK’s most prolific supplier of retail facial recognition technology, has announced its intention to extend its services into the pharmacy sector.¹ In practice, this means facial recognition scans of those accessing NHS treatment. We are concerned that, should pharmacies begin deploying this intrusive biometric surveillance technology, it will have profound consequences for privacy and discourage people from seeking health care: particularly the most vulnerable.

We therefore urge the Committee to take evidence on the potential impact that the use of LFR in NHS affiliated pharmacies.

LFR operates by detecting the face of every person that walks in range of the camera and creating a unique biometric template from their facial features. This template is then compared against a pre-prepared database of images known as a ‘watchlist.’ If the LFR system detects a match between an individual entering the shop and an image on the watchlist, the shop staff or security will receive an alert.

Facewatch functions as a form of privatised policing system. Decisions about who is placed on a watchlist are made at the discretion of shop staff rather than the police or the courts, with no requirement that any threshold of criminality be met, no obligation to report the alleged offence to the police and no minimum standard of evidence or investigation. People who are placed on watchlists have no right to be informed of their inclusion and typically only discover it when they are stopped on subsequent

¹ Press Release, ‘Facewatch invites pharmacy operators to see how live facial recognition can prevent rising theft and protect staff from abuse,’ 28 May 2026, <https://www.facewatch.co.uk/facewatch-invites-pharmacy-operators-to-see-how-live-facial-recognition-can-prevent-rising-theft-and-protect-staff-from-abuse/>.

visits or refused entry. Those who are flagged by the system have no trial process and no route to appeal, making it difficult to challenge.

By design, LFR systems cannot limit the members of the public they scan to those individuals suspected of wrongdoing. Instead they detect and process the facial biometric data of every person who enters the store. Facial biometric data is highly sensitive personal information, comparable to fingerprints or DNA.

The implications of LFR are particularly grave in healthcare settings, which engage some of the most sensitive and private aspects of our lives. Requiring every customer to submit to a biometric identity check at pharmacy doors will, we believe, deter many people from seeking important, potentially life saving healthcare. This could affect families, children, pregnant women, and those accessing contraceptive services and is particularly dangerous for vulnerable patients including those who are elderly or disabled who often have serious health needs but cannot easily travel elsewhere.

This risk is only exacerbated by the reality of innocent people being wrongly flagged by LFR or unfairly included on watchlists. Big Brother Watch is regularly contacted by members of the public who have found themselves wrongly blacklisted, publicly accused of theft, thrown out of stores and humiliated due to LFR mistakes, as documented by the *BBC*² and *The Guardian*.³ There are also well-documented concerns about bias and accuracy in facial recognition technologies. These statistical conclusions are supported by anecdotal evidence. In 2024, Big Brother Watch assisted a woman of colour to take legal action against Facewatch after she was misidentified in Home Bargains, publicly accused of theft and banned from all major retailers who used Facewatch's technology. Facewatch subsequently admitted that her identification had been the result of an error.⁴

In other retail contexts, there is evidence that innocent individuals have been added to watchlists by security staff for malicious reasons when they have done nothing wrong.⁵ If this behaviour is replicated in the healthcare setting, it would have devastating effects. As Facewatch shares its watchlists with other subscribing retailers in the area, wrongly flagged individuals may find that they are blacklisted not

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

3 The Guardian, 'Guilty until proven innocent: shoppers falsely identified by facial recognition system struggle to clear their names,' 3 May 2026, <https://www.theguardian.com/technology/2026/may/03/guilty-until-proven-innocent-shoppers-falsely-identified-by-facial-recognition-struggle-to-clear-their-name>.

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

5 The Guardian, 'AI facial recognition oversight lagging far behind technology, watchdogs warn,' 3 May 2026, <https://www.theguardian.com/technology/ng-interactive/2026/may/03/ai-facial-recognition-oversight-lagging-far-behind-technology-watchdogs-warn>.

only from the store where the initial error was made, but also all other participating stores.

We urge the Committee to take evidence on:

- What impact the use of this technology would have on the public's access to healthcare.
- What differential impact the use of this technology would have for vulnerable groups accessing healthcare.
- What assessment Facewatch has made of these questions and, if they believe the technology will have an impact.

Yours sincerely,

Silkie Carlo
Director, Big Brother Watch