FACEWATCH ADDRESSES MISLEADING AND FALSE CLAIMS MADE BY PRIVACY GROUP IN LEGAL COMPLAINT

Big Brother Watch claims supermarket biometric scans of "thousands of shoppers" is "unlawful" and "Orwellian in the extreme". Shoppers can be spied on, blacklisted across multiple stores, and denied food shopping despite being entirely innocent".

Orwellian? What? To use a new technology that works for retailers to protect their employees, customers and assets?! A misleading statement designed to create concern and fear. However, there is a fundamental difference between shoppers and abusive thieves. Shoppers pay for their goods, thieves don't and therefore are not "innocent shoppers". Facial recognition is lawful for the purpose of crime prevention under the Data Protection Act if the strict criteria set out are followed – Facewatch operates in full adherence with the law.

First known legal complaint against facial recognition in retail urges new Information Commissioner to investigate and "stop unlawful processing"

Facewatch has always been open and collaborative with the ICO and welcomes any further constructive feedback from them as we take our responsibilities around the use of facial recognition extremely seriously. We work hard to balance our many retail clients' customers rights with the need to protect their staff and customers from unacceptable violence and abuse across the UK.

Facewatch also uses photos of innocent shoppers to "improve its system"

This is untrue. Facewatch do not collect images of shoppers to improve our system.

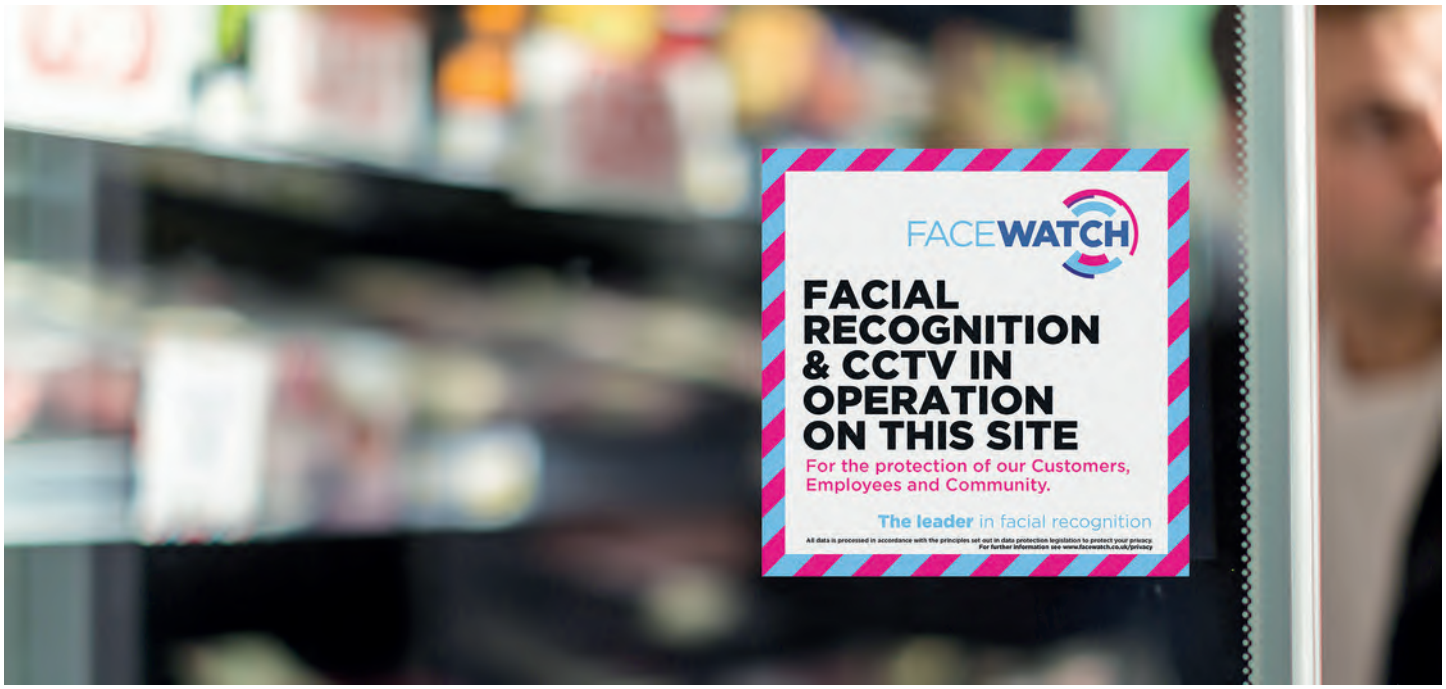
Privacy rights group Big Brother Watch has filed a legal complaint with the Information Commissioner claiming that Southern Co-operative's use of live facial recognition cameras in its supermarkets is "unlawful". The legal complaint, sent via the group's lawyers from data rights firm AWO, claims that the use of the

biometric cameras "is infringing the data rights of a significant number of UK data subjects". The legal complaint outlines how the system, sold by surveillance firm Facewatch, "uses novel technology and highly invasive processing of personal data, creating a biometric profile of every visitor to stores where its cameras are installed." The supermarket chain has installed the controversial surveillance technology in 35 stores across Portsmouth, Bournemouth, Bristol, Brighton and Hove, Chichester, Southampton, and London. The supermarket's staff can add individuals to the facial recognition "blacklist", making them a "subject of interest". Shoppers are not informed if their facial biometric data, similar to the data held on modern passports, is stored or added to the supermarket's blacklist where it is kept for up to two years.

Clear signage is in place across all Facewatch protected stores. Biometric data is not retained for shoppers, it is deleted instantaneously. The only biometric data that is retained is for people who are reasonably suspected of committing crimes in the stores, which is retained for 1 year (not 2). The data is retained so we may generate an alert to subscribers when the offender enters their premises.

According to the Southern Co-operative's correspondence with Big Brother Watch, staff do not receive photos from or give photos to the police, but rather use the biometric profiles to create an alert if certain shoppers enter the store and to share allegations of unwanted conduct between staff in different stores.

Facewatch does not accept reports of "unwanted conduct" there has to be documented evidence of a crime having been committed in their stores accompanied by a digitally signed witness statement.



Photos of shoppers who are not on any watchlist may be kept for days for Facewatch to "improve its system", according to Facewatch documents analysed in the complaint.

Facewatch retain CCTV stills like any other CCTV system in order to be able to identify and report crimes that have already happened. Facewatch do not collect images of shoppers to improve our system. Facewatch CCTV images (not biometric images) are retained for only 5 days, whereas most CCTV operators retain footage for 30 days.

The privacy NGO's legal complaint claims that this biometric surveillance poses "significant" risks to to shoppers' rights and freedoms.

The privacy intrusion to genuine shoppers is negligible. Indeed, the Court of Appeal ruled in Ground 2 of the Bridges v South Wales case that the use of AFR was proportionate and did not contravene individual rights because the impact on every member of the public was as "negligible as that on the Appellant

himself", that is "near instantaneous algorithmic processing and discarding of biometric data". This is exactly what Facewatch does.

Southern Co-operative supermarkets use facial recognition software with surveillance cameras from Chinese state-owned firm Hikvision, which also provides cameras for the CCP's concentration camps in Xinjiang and has been associated with serious security flaws. The firm is banned from operating in the US and a group of senior parliamentarians recently urged the Government to ban the cameras from the UK.

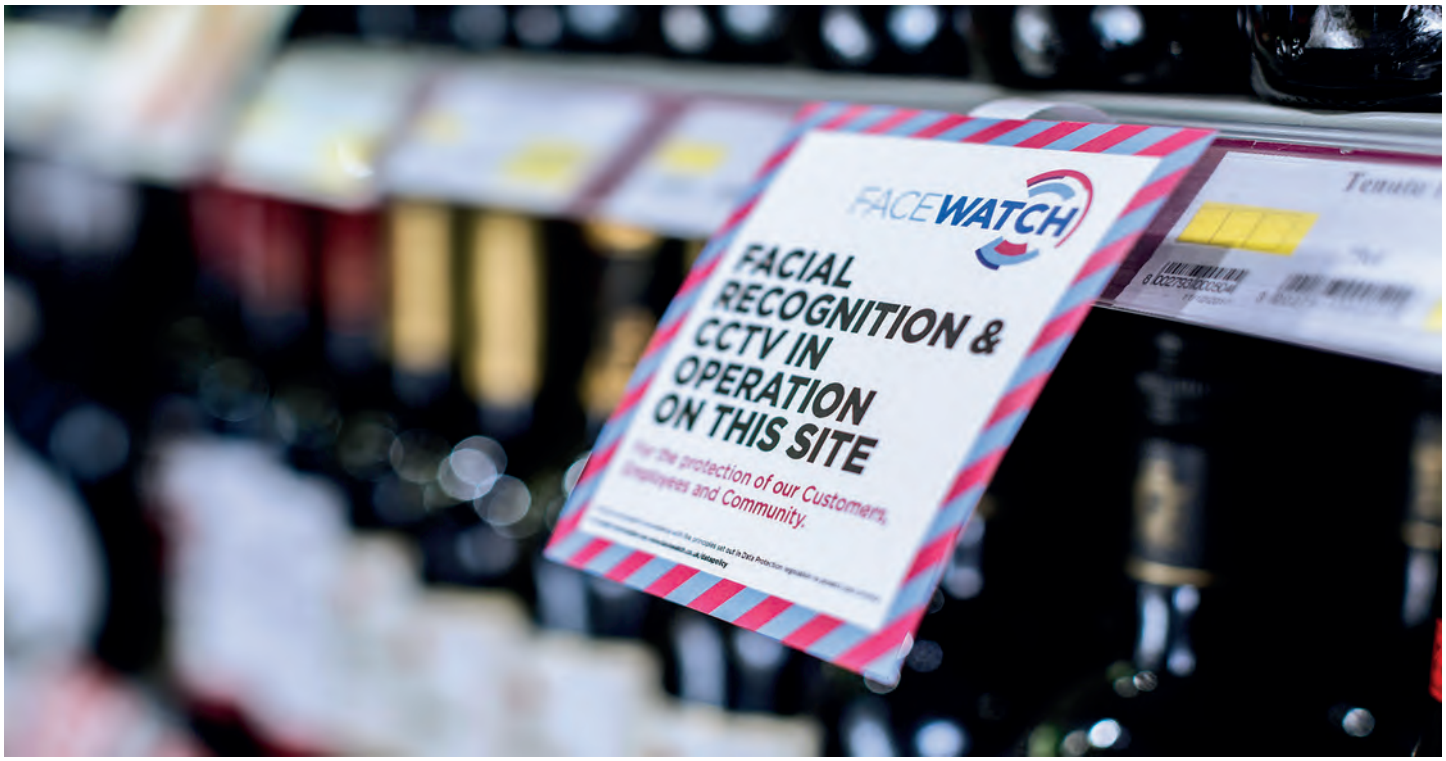
Facewatch do not use Chinese facial recognition software provided by Hikvision or any other Chinese algorithm provider. We use algorithms from two leading NIST (National Institute of Standards and Technology) accredited US companies. Facewatch use standard CCTV cameras from various major hardware providers and in Southern Coops case there are two camera manufacturers products. Facewatch are agnostic to the hardware and will follow the Government's lead on whether to continue using Hikvision hardware or not.

The facial recognition software used with the cameras, provided by UK firm Facewatch, can be used to share biometric photos of "subjects of interest" with other companies that buy access to their system. Subjects of interest photos can be shared in an 8 mile radius from where they are taken from stores in London, or up to a 46 mile radius in rural locations.

Our sharing of images is only of witnessed and evidenced offenders and complies with the principles of data minimisation and proportionality.

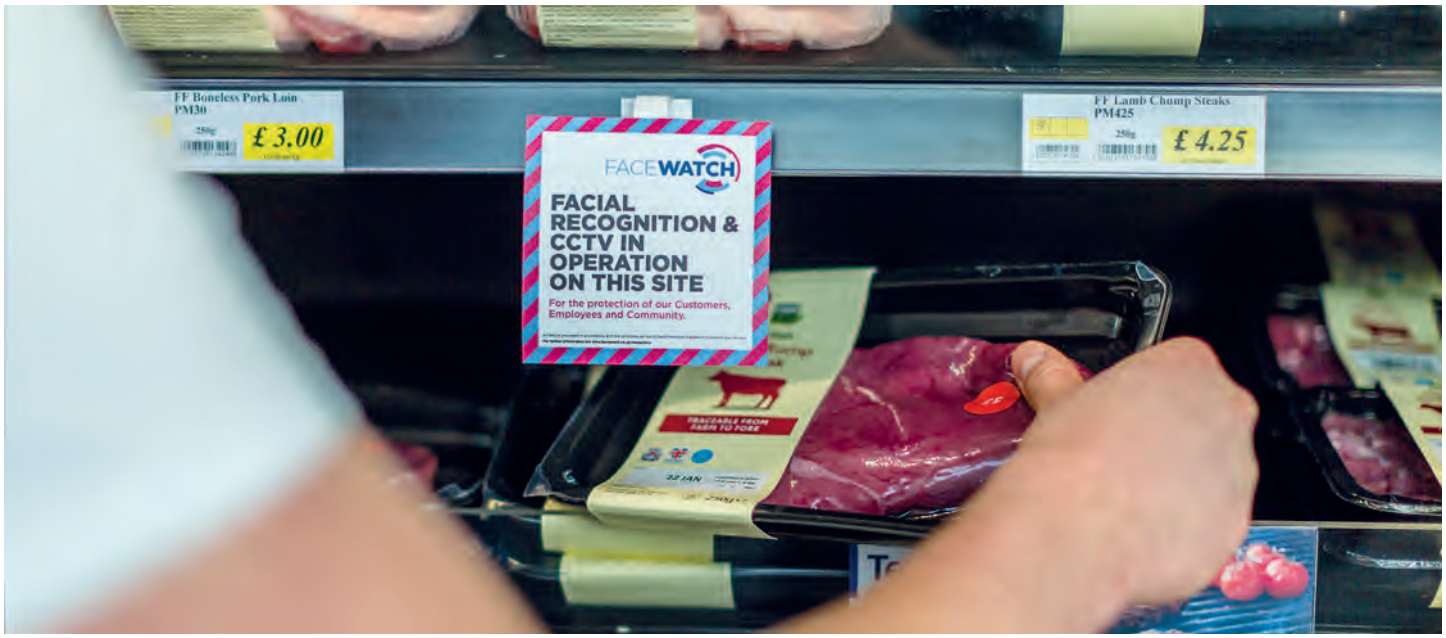
Being on the watchlist for one of Facewatch's clients like the Southern Co-operative could have serious detrimental impacts on someone's day to day life. BigBrother Watch is urging anyone who thinks they might have been affected by this to reach out to them, as they may be able to challenge their inclusion on the watchlist.

As noted above ONLY individuals reasonably suspected of having committed offences are on the watchlist, not regular shoppers. Even if you are on the watchlist the only impact as stated by the Southern COOP is: 'Any shopper previously banned would be asked to leave, and others would be approached by staff with an offer of "how can I help?" to make it clear their presence had been detected'. Our aim is to deter reoffending.



Live facial recognition has been the subject of growing controversy in recent years, with moves in the US and EU to ban the technology from being used for public surveillance. Research shows that the technology can be highly inaccurate, particularly with people of colour and women. Big Brother Watch's research found that 87% of facial recognition "matches" in the Metropolitan Police's trials of the surveillance technology in fact misidentified innocent people.

Facewatch only uses algorithms independently tested as highly accurate. This description of data accuracy is for police use and is over 4 years old and warrants no response, especially as the figures quoted then were in fact contested as inaccurate by the Police even then FR algorithm quality has improved 30 fold since 2019. Please refer to the NIST site which contains full details of current algorithm quality in a definitive and properly evidenced set of data.



QUOTES

Silkie Carlo, director of Big Brother Watch said:
"Our legal complaint to the Information Commissioner is a vital step towards protecting the privacy rights of thousands of people who are affected by this dangerously intrusive, privatised spying.
"The Southern Co-op's use of live facial recognition surveillance is Orwellian in the extreme, highly likely to be unlawful, and must be immediately stopped by the Information Commissioner.
"The supermarket is adding customers to secret watchlists with no due process, meaning shoppers can be spied on, blacklisted across multiple stores, and denied food shopping despite being entirely innocent. This would sound extreme even in an episode of Black Mirror, and yet it is taking place right now in Britain.
"This is a deeply unethical and frankly chilling way for any business to behave and I'd strongly recommend that people do not shop at the Southern Co-op whilst they continue to spy on their shoppers."

Nick Fisher, CEO of Facewatch said:
"Facewatch is a vital tool for UK retailers, and significantly reduces crime, violence and anti-social behaviour wherever it is deployed. Our customers have turned to us after other methods of crime prevention such as CCTV, police, tagging and manned guarding have failed.
BBW put out misleading, false and alarmist information which is designed to create fear in the general public by demonising the use of facial recognition technology. For example, we do not share the faces of shoppers - only images of witnessed and evidenced offenders, nor do we use Chinese algorithms.
Facial recognition is lawful for the purpose of crime prevention under the Data Protection Act if strict criteria are adhered to. Facewatch operates in full adherence with the law. Facewatch has always been open and collaborative with the ICO and welcomes any further constructive feedback from them as we take our responsibilities around the use of facial recognition extremely seriously."

Alex Lawrence-Archer, Solicitor at data rights agency AWO said:
"Our legal analysis shows there are good reasons to believe that Facewatch and Southern Co-op's implementation of live facial recognition technology is in breach of data protection legislation. And it could be causing serious harm to people on their 'watchlists'.
"This kind of high-risk, biometric processing needs a strong justification, and it's not at all clear that Facewatch and Southern Co-op meet that test.
"We also highlight significant risks of unfair bias and inaccuracy in the implementation of the system, both of which further suggest that it is unlawful.
"Our data rights can give us a say in whether and how companies can use technology to exercise power over us, but only if they are enforced. That is why it's urgent that the ICO investigates this system."

Dean Armstrong, QC says:
How Facewatch complies with the DPA
Facewatch as data controller shares and processes Personal Data, Special Category Personal Data and Criminal Offence Data with its business Subscribers. The Data Protection Act 2018 provides that such processing and sharing is justified if certain conditions are met.
In Mr. Armstrong QC's opinion, Facewatch satisfies those conditions because: (1) it is necessary to provide alerts to business subscribers to prevent or detect unlawful acts; (2) such processing cannot be carried out with consent as it relates to crime prevention; and (3) because Facewatch is processing data on a national level and is demonstrated to reduce/prevent crime in subscriber properties with the further potential to prevent and detect crime it is in the Substantial Public Interest.