Mark Smith
Chief Executive Officer
Southern Co-operative

Sent by email: press@southerncoops.co.uk

CC:
dataprotectionofficer@southerncoops.co.uk

01 December 2020

Dear Mr Smith

We are writing to voice our serious concerns and call for urgent assurances regarding the use of Facewatch facial recognition cameras in your stores.

Privacy International (PI) campaigns against companies and governments who exploit our data and technologies. We expose harm and abuses, mobilize allies globally, campaign with the public for solutions, and pressure companies and governments to change.

Southern Co-op use of Facewatch

In an article on Facewatch's website posted on 5th October 2020[1], a Loss prevention officer at the Southern Co-op confirmed that "we have completed a successful trial using Facewatch [facial recognition] in a select number of stores" to alert "our store teams immediately when someone enters their store who has a past record of theft or anti-social behaviour".

It is not known how many stores the system was used in, or if there are imminent plans to roll out the system to further stores. Given the characterization of the trial as "successful" however, we could potentially infer that there seem to be at least no plans to stop using the system.

Facewatch

[1] https://www.facewatch.co.uk/2020/10/05/facewatch-at-the-southern-co-op/

Facewatch Limited describes itself as a "cloud-based facial recognition security system [which] safeguards businesses against crime."[2] Premises using the system are alerted when Subjects of Interest (SOI) enter their premises through the use of facial recognition cameras. Facewatch's privacy policy states that subscribers "are able to report new SOIs through incidents which include a formal witness statement."[3] Facewatch has "a National Watchlist of Subjects of Interest" which allows them to then "create a personalised watchlist for every one of our customer's properties individually."[4] In addition to an alert system, Facewatch allows premises to run analytics through their customers, including by gender and ethnicity.[5]

Potential sharing with police

According to the FT, in 2019[6], "Facewatch [was] about to sign data-sharing deals with the Metropolitan Police and the City of London police, and [was] in talks with Hampshire police and Sussex police".

According to the founder of Facewatch, Simon Gordon, "The deal with police is they give us face data of low-level criminals and they can have a separate watchlist for more serious criminals that they plug in…" If the systems spot a serious criminal, the alert is sent directly to the police, rather than to retailers, according to the FT.

PI is not aware whether Facewatch has in fact entered into any such agreements with any UK police force, and has not received a response from Facewatch when we asked the company in both June and September 2020.

However, Facewatch has uploaded a template Information Sharing Agreement (ISA) to the government G-Cloud system, which states "Based originally on Met Police Template."[7] As explained in the ISA:

---

[2] https://www.facewatch.co.uk
[3] https://www.facewatch.co.uk/privacy/
[4] https://www.facewatch.co.uk/privacy/facewatch-and-gdpr/
[5] https://assets.digitalmarketplace.service.gov.uk/g-cloud-11/documents/92526/211868666506697-service-definition-document-2019-04-10-1043.pdf p13
[6] https://www.ft.com/content/605de54a-1e90-11e9-b126-46fc3ad87c65
[7] https://assets.digitalmarketplace.service.gov.uk/g-cloud-11/documents/92526/211868666506697-terms-and-conditions-2019-04-10-1045.pdf

"Facewatch also enables the Police to upload images to the Watchlist and be alerted to Major Crime SOIs and Missing Persons if they enter Subscriber Premises. These Major Crime SOI's and Missing Person SOI's and any alerts related thereto ***are not shared with Facewatch Subscribers.*** *[emphasis added]"*

The ISA envisages further the use of a segregated watchlist system only available to the police. This would in effect transform what is a retail crime alerting system into an extensive, potentially nationwide, police facial recognition surveillance system.

As of March 2019, Facewatch pricing list[8] makes clear:

"Police may upload Subjects of Interest for Major crime, CT incidents knowing that this is completely secure and under their control as they will manage the cloud servers hosting the segregated system.

Algorithmic probes from cameras sited in Facewatch Subscriber properties of all persons entering will be sent to the segregated system to compare against the police confidential watchlist.

Police will receive alerts to specified users.

Police will also have access to the main Facewatch business system to search for intelligence (eg Stop and Search, take a photo to see if individual is on Police or Business system)."

The ISA clarifies how this system would work:

"In a segregated system Police are provided with a stand-alone copy of the Facewatch system in a segregated cloud server under their own control. Only Police can upload, view and remove SOI's in this server.

[8] https://assets.digitalmarketplace.service.gov.uk/g-cloud-11/documents/92526/211868666506697-pricing-document-2019-04-10-1138.pdf

Facewatch will transmit Probes of individuals entering Subscriber premises directly to the segregated system. The Probes are compared to the segregated system watchlist(s) and if there is a match the segregated system requests the "just seen" image from the Edge Equipment and an alert is sent to Police showing the watchlist image and the just seen image with a percentage match score. If there is no match the Probe is deleted immediately from the segregated system."

The ISA outlines the sharing of three types of batch data. Category A, Low risk, would allow Police to upload "images extracted from *Police* custody imaging system, CCTV or Body Worn Camera footage of individuals… who are believed to be committing criminal acts within the area and are considered low risk." Category B would allow *Police* to upload images to separate police watchlist(s) in a segregated system which only alert *Police*, and would cover more serious crimes. And Category C would allow police to "create watchlists for their own purposes without reference to Facewatch.

Facewatch makes clear that Police authorities may also use the system as an intelligence tool:

"Police may use Alerts and information available by logging into the Facewatch system to identify SOIs and to support enquiries, operations and crime prevention. Police will consider the application of relevant legislation to the circumstances."

Concerns

We are concerned both by the Southern Co-op's decision to deploy facial recognition cameras -even at trial level- in its stores as well as the potential use of the cameras to share data with police.

As you are aware, the ongoing coronavirus pandemic has highlighted the key role played by retail staff in our communities who have, at significant risks to themselves, continued to provide essential services including to vulnerable members of communities.

Given the vital importance of access to stores such as Co-op during lockdown, we are concerned that, in order to purchase essential goods, people might be in effect left with no

choice but to submit themselves to facial recognition scans. Given the need to buy essential goods and lack of viable alternatives in many communities, they may have no other choice and therefore cannot in effect provide valid, unambiguous, explicit and freely-given consent to such capture of their sensitive personal data, as required by data protection laws. Further, the use of such cameras may deter people accessing vital goods who may have a criminal record or simply be concerned they might be listed in a watchlist, for fear they will be flagged to staff and very publicly refused entry to the store.

We are also deeply concerned about the potential sharing of captured data with police, with or without Co-op's knowledge.

If such a system were to be widely deployed it would be a radical extension of the police's surveillance powers. It would extend police use of live facial recognition into every participating Southern Co-op shop.

The outsourcing of facial recognition to the private sector in such a way would enable the surveillance of drastically higher amounts of people while offering them less legal safeguards. For example, the Metropolitan Police have so far insisted[9] that use of facial recognition would be at "specific locations…focused on a small, targeted area… clearly signposted [and] not linked to any other imaging system, such as CCTV, body worn video or ANPR [i.e. Automatic number-plate recognition]."

Such a network would give police access to drastically more facial recognition cameras, raising urgent questions around transparency, legality, necessity and proportionality. While the deployment of facial recognition by police may in some circumstances be clearly signposted, it is not clear if this will be the case if the police use Facewatch's system, as it is questionable whether the use of the latter can abide by existing legal frameworks.

Assigning pre-emptive policing functions or endorsing the existence of private surveillance networks distorts long-established societal premises of privacy and perceptions of authority. In absence of a precise and public legal framework, as well as clear safeguards, the existence

[9] https://techcrunch.com/2020/01/24/londons-met-police-switches-on-live-facial-recognition-flying-in-face-of-human-rights-concerns/?guccounter=1

of facial recognition networks will inevitably blur the lines between public and private spaces, allowing for the erosion of our privacy rights, but also fundamental freedoms.

Request

Given these concerns we are writing to ask that you confirm:

- Whether Southern Co-op has reviewed any privacy as well as any other fundamental rights concerns related to the use of Facewatch, and if so, what the outcome of that review was;

- Whether you believe the legal framework governing your stores' use of Facewatch is currently sufficiently clear and able to satisfy the requirements of clarity, foreseeability and accessibility as well as the legal tests of necessity and proportionality under the GDPR and the UK Data Protection Act 2018. We note there is no mention of Facewatch in Co-op Southern's privacy notice[10];

- Whether you are aware if Facewatch has in fact entered into such a data sharing agreement with any Police force or whether it is sharing any data with Police, or whether it is likely to in the near future.

    - If not, whether you will investigate the matter and confirm with Facewatch if it is or has shared data collected in your stores with any Police force, or if it has allowed any Police force access to the cameras, or if it has any plans for doing so.

We would like to thank you for your attention to this matter and would like to take the opportunity to congratulate and thank all your staff for providing essential support to communities during this pandemic. We are mindful of the challenging commitments your stores face at the moment and are keen to ensure they continue to support communities in line with Southern Co-op's principles[11].

[10] https://www.thesouthernco-operative.co.uk/wp-content/uploads/SC-Website-Privacy-Notice.pdf
[11] https://www.thesouthernco-operative.co.uk/about-us/#tab-id-3

We would appreciate a response at your earliest convenience.

Yours sincerely,

Edin Omanovic

Advocacy Director