

11th December 2020

Edin Omanovic
Advocacy Director
Privacy International
62 Britton Street
London
EC1M 5UY

Dear Mr Omanovic

Your letter dated 1st December, addressed to Mr Smith, our Chief Executive, has been passed to me for response.

We have noted the contents of your letter and the specific questions you have raised, answers to which are provided below:

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.

Yes, Southern Co-op followed the requirements of GDPR and the Data Protection Act 2018 in relation to its trial of facial recognition technology. Our impact assessment determined that the use of this technology did not create a high risk to the rights and freedoms of data subjects.

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.

Already this year we have seen an 80 percent increase in assaults and violence against our store colleagues. This is not acceptable. We're working hard to protect them but this is not at the expense of our customers' rights.

We have more than 200 stores across the south and have focused the use of facial recognition in 18 branches where there is a higher level of crime. The system is GDPR compliant and does not store images of an individual unless they have been identified as a repeat offender.

The purpose of our limited and targeted use of facial recognition is to identify when a known repeat offender enters one of our stores. This gives our colleagues time to decide on any action they need to take, for example, asking them politely to leave the premises or notifying police if this is a breach of a banning order. All of our customers at the 18 stores have been made aware with distinctive signage.

The number one reason for violence in our stores and within the wider retail sector is when a colleague intervenes after a theft has already taken place. Using facial recognition in this limited way has improved the safety of our store colleagues.

No facial images are shared with the police or with any other organisation, nor are any other organisation's images shared with us for use within facial recognition. Only images of individuals known to have offended within our premises, including those who have been banned/excluded, are used on our facial recognition platform. Only the image of the known offender is stored in the platform. No sensitive data in relation to those persons is held. The platform does not store the image of every person who enters our store.

Any further use of facial recognition will be limited and we have no plans to roll this out across all of our stores.

We therefore do believe that our use of the system meets the tests of being necessary and proportionate.

The way in which we use any personal data across our business is set out in our Privacy Notice [and ancillary policy notices]. We have a legitimate business interest to use facial recognition to protect the safety of our colleagues and customers. Across our business we work with subcontractors who provide services where we do not have the expertise in house, as set out in our Privacy Notice, and, as is common practice, we do not refer to all of these subcontractors individually by name as it would not be practically possible to keep the Privacy Notice up to date. Signage is displayed in the stores that are currently using facial recognition technology.

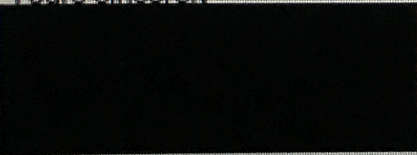
Whether you are aware if Facewatch has in fact entered into such a data sharing agreement with any Police force or whether it is sharing any data with Police, or whether it is likely to in the near future.

We have no such knowledge.

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 have no current plans to investigate the matter. The system that we operate is standalone and contains only images of evidenced offenders that we have authorised to be held in the system. Such images are not shared with the Police or any other third party.

Yours sincerely



Data Protection Officer