Published on *The National Law Review* https://natlawreview.com

The Southern Co-op – Is the Use of 'Spy' Cameras Breaching UK Data Protection Laws?

Article By:

Malcolm Dowden

The UK convenience store giant 'Southern Co-op' is facing the possibility of regulatory intervention and legal challenge following a complaint made by UK civil liberties campaign group Big Brother Watch (BBW) regarding the use of surveillance cameras in 35 Southern Co-op stores. Images of customers that a member of staff 'reasonably expects' to be committing 'crime or disorder' are captured and transformed into biometric data. The data of those 'identified as an offender' is then stored and checked against the database of facial recognition technology provider, 'Facewatch.'

BBW argue that Southern Co-op use 'highly invasive' methods of surveillance to 'create and enforce *ad hoc* and dynamic blacklists of individuals they wish to exclude from their stores.' BBW director, Silkie Carlo, said that '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.' Southern Co-op argue that the security 'system is GDPR compliant' and that the safety of both their customers and colleagues is 'paramount.'

Under Article 6 UK GDPR, the processing of personal data is only lawful if one or more of the six lawful bases apply. Southern Co-op rely on Article 6(1)(f) UK GDPR and view the processing as necessary for the purpose of their legitimate interests (namely to protect their business against criminal activity and to protect the safety of colleagues and customers). However, to be lawful this must be balanced against the 'interests or fundamental rights and freedoms of the data subject.' Although not published, when questioned on their specific legitimate interests, Southern Co-op revealed that they have undertaken a legitimate interest's assessment which found that they can rely on Article 6(1)(f) as their lawful purpose. Nonetheless, BBW believe that their reasoning is insufficient, 'less privacy-intrusive approaches' have been 'ignored' and that the interests of the data subjects should prevail.

Southern Co-op and Facewatch also claim to meet a condition for permitted processing special categories of personal data (which includes biometric data), which would otherwise be prohibited under Article 9 UK GDPR. However, BBW assert that the processing falls short of the conditions set out in the Data Protection Act 2018 Schedule 1 because it is 'not necessary for crime prevention, and it is not in the substantial public interest.' ICO guidance about what would satisfy the requirement of 'substantial public interest' explains that 'vague or generic' public interest arguments are insufficient; organisations 'should be able to make specific arguments about the

concrete wider benefits' of their processing. BBW believe that Southern Co-op use facial recognition software 'as a means of more general access to control stores, not exclusively to prevent or detect unlawful acts.' The campaign group go as far as suggesting that Facewatch and Southern Co-op's interest is wholly private in nature and therefore not in the public interest, let alone in the 'substantial' public interest.

In their complaint submission, BBW make reference to *R (Bridges) v South Wales Police* [2020] EWCA Civ 1058 in which the Court of Appeal held that automated facial recognition technology used by South Wales Police breached data protection laws and Article 8 of the European Convention on Human Rights. In their view, the processing in Southern Co-op's stores is 'significantly more intrusive' than in *Bridges*. However, *Bridges* did not completely rule out the use of facial recognition technologies, provided that sufficient data protection impact assessments and thorough policy documents are established.

Whether the use of 'spy' cameras in Southern Co-op stores is breaching data protection laws is yet to be decided. The ICO's response is likely to be eagerly awaited by other organisations such as Sports Direct, Spar and Nisa – who also use Facewatch's services. Should the ICO find that Southern Co-op or Facewatch have breached data protection laws, they could face substantial fines or other enforcement measures such as a "stop notice" barring the use of facial recognition technology.

This article was co-authored with Ellie Phillips (University of Winchester).

National Law Review, Volume XII, Number 208