Browne Jacobson

Cameras in convenience stores: a potential hornet's nest..?

A convenience retailer has opted to install cameras (the "Facewatch" system) at a limited number of its English stores to reduce crime and protect its staff.

24 August 2022

A convenience retailer has opted to install cameras (the "Facewatch" system) at a limited number of its English stores to reduce crime and protect its staff. You might say, so what?

Well, this decision has been challenged by a privacy campaign group (Big Brother Watch) because of how the cameras work and what they say the retailer does with the footage / images they capture.

Use of facial recognition cameras, biometric data or even CCTV cameras in public places or retail forecourts by local authorities and landlords is nothing new, nor is it necessarily against English data privacy laws. Relevant users of the systems (the data controller and/or processor) must be able to demonstrate (which they should document, typically through a written impact assessment) that such use is a proportionate means of achieving a legitimate aim. This could include the detection and prevention of crime or the protection of public safety in locations where crime has become a concern and the same objective cannot reasonably be achieved by other, less privacy intrusive means. In this case, visible notices should be places in those areas so that the public (data subjects) are aware that they are being filmed and their images are being processed. The relevant data controller / processor then needs to ensure they are registered with the data protection regulator (the Information Commissioner's Office / ICO) to process such data each year.

In this case, the retailer says that the camera captures faces of customers. Images are then analysed against the retailer's database of people who (the retailer says) have perhaps previously stolen from its stores or been violent or abusive to staff. These people did not necessarily have criminal convictions. On that basis, it goes further than traditional CCTV cameras. In contrast, the privacy campaign group is concerned that people who do not actually have any criminal convictions could be added to a secret "watch-list" and denied access, despite possible innocence. They also argue it doesn't bring criminals to justice; instead, it just displaces crime and empowers individual businesses.

Any retailer is entitled to refuse to serve, or deny access, to anyone. This system will (it will claim) help it to identify those whom it has a legitimate interest in doing so. The retailer will also be able to argue that if you don't behave inappropriately or unlawfully, then this system will not affect you.

ICO decision is awaited. The ICO may respond and determine that the retailer has complied with data protection laws and followed ICO guidance on installation of the system and processing of its data (in which case, it is up to shoppers whether they wish to continue to use such stores). If so, the retailer may continue to use the system and may consider rolling it out across other stores with similar problems. Other retailers may also adopt similar systems in future.

Alternatively, the ICO may determine that the system itself may not be unlawful, but the retailer was not using it correctly, in which case it can ask the retailer to decommission the system (either permanently or temporarily) and cleanse its databases until it can do so. Other sanctions may follow in addition.

Finally, if the ICO determines that such a system is unlawful, then the retailer could receive monetary enforcement notices and/or potential class action claims from data subjects who have been improperly recorded by the system. Associated reputational damage and potential decline in customer footfall may also follow.

Our view is that unless the ICO can find that the system is not being used properly, or was not implemented in a compliant manner, and the retailer can justify why traditional CCTV was not appropriate for this specific problem, then the ICO is more likely to side with the retailer on this one.

ICO decision is awaited. This is likely to be of major interest to retail and hospitality providers, operators of public spaces or education centres who are either considering implementing facial recognition systems to tackle a specific problem or are already doing so. For now, if you are using such a system, be sure to document your impact assessment ready for disclosure to the ICO if a complaint arises, and make sure you are correctly registered with the ICO to do so. If you have a specific problem you want to address, and you think that such a system may be the way to go in tackling that, then you should seek legal advice and await the ICO's decision before doing so.

Contact

Sarah Parkinson

Partner

sarah.parkinson@brownejacobson.com

+44 (0)115 976 6575

Related expertise

Commercial law