ICO ISSUES OPINION ON THE USE OF LIVE FACIAL RECOGNITION BY LAW ENFORCEMENT

The first Opinion under DP Act 2018 has been issued by the UK's Information Commissioner (ICO). Aaminah Khan, Barrister, analyses the issues at stake.

The Opinion sets out the ICO's position and makes recommendations relating to the use of Live Facial Recognition by police forces, following an ICO investigation into how the police use this technology in public spaces. A report of the ICO investigation findings, together with the Opinion, were both published on 31 October 2019. Considering that this is the first Opinion issued by the Commissioner under section 116 and Schedule 13 of the Data Protection Act 2018, since the commencement of the Act, shows how high of a priority this topic is for the ICO.

Live facial recognition technology processes, in real time, biometric data, allowing police to identify individuals as they pass facial recognition cameras, although non-live methods of identification, i.e. from older or still images are also utilised by the police. As it involves the processing of biometric data, live facial recognition is brought within scope of GDPR and the DP Act 2018, with police forces having to comply with Part 3 of the DP Act 2018. The use of live facial recognition by law enforcement constitutes sensitive processing of biometric data under section 35 of the Act and as such is subject to greater safeguards under the Act, for example the police have to demonstrate that the processing is strictly necessary, rather than merely necessary, and further that a Schedule 8 DP Act 2018 condition is met. The use of this technology by police forces in recent times has been on the increase, having been used at events where large crowds of people are expected such as football stadiums and the Notting Hill Carnival.

Whilst this Opinion, the investigation and its recommendations focus on law enforcement, many of the privacy issues that this developing technology raises will come into play when the use of this technology is being considered by the private sector. It is clear that there is a growing interest from private sector organisations in facial recognition type technology, from shopping centres wanting to identify known shoplifters or individuals with retail exclusion orders to bars and nightclubs wanting to identify persons of interest, and it is easy to see why the use of facial recognition may be attractive to some businesses. It is also clear that this technology is a

regulatory priority for the ICO, who have indicated that they are also investigating its use outside of the policing sphere.

The ICO report and Opinion follow a 17-month investigation into the use of live facial recognition by primarily South Wales Police and the Met Police Service. Aside from the ICO investigation, for several months Facial Recognition Technology (FRT) has also featured regularly in the media, from Kings Cross Estate using FRT for almost two years without the public being aware, to debate around the increasing use of FRT in shops and supermarkets.

During the course of the ICO's investigation, the use of FRT by South Wales Police led to the case of *R (Bridges) v Chief Constable of South Wales Police and Others*[1]. South Wales Police trialled live facial recognition technology in public spaces, in order to identify individuals who may be connected to criminal activity or at risk in some way, by scanning profiles and comparing against offender databases.

The technology processes the biometric data of potentially thousands of individuals who pass before the cameras. Some individuals will be stopped and spoken to by officers as a result, sometimes without justification, as the accuracy and effectiveness of the technology has been questioned, particularly in relation to some ethnic groups. The action of South Wales Police was challenged by way of Judicial Review in the case of *Bridges* by a member of the public, concerned about the lawfulness of the way his data had been processed.

The High Court in *Bridges* did not consider that the processing was unlawful, rejecting the claimant's arguments that the processing carried out by South Wales Police was not in accordance with the law or proportionate. However the claimant has publicly confirmed that they have commenced an appeal against the decision.

With the lawfulness of South Wales Police's use of FRT being confirmed by the High Court, subject to any appeal, it is likely to continue to be rolled out and increase in prevalence. One of the main recommendations in the Opinion is the Commissioner's call for the strengthening of the legal framework in this area, in order for there to be greater clarity, foreseeability and consistency in relation to the use of the technology, by the introduction of a statutory Code of Practice. A statutory code would no doubt be welcome by many, as it would provide a clear framework for data controllers on how to carry out this processing in a way that is justifiable and proportionate, especially as this is one of the areas of developing technology where the legal

[1] [2019] EWHC 2341 (Admin)

framework and guidance is struggling to keep pace with the speed of technological advancement taking place.

With FRT such a contentious issue, this will be an area the ICO is expected to keep a close eye upon, and it may only be a matter of time before formal enforcement action is taken by the ICO in this area. Certainly, given the warnings from the UK Commissioner on how concerned she is about this issue, any data controller planning FRT who does not take compliance with the DPA and GDPR seriously ought not to be surprised if they find themselves subject to an ICO investigation.

The full version of this article is published in Privacy Laws & Business, UK issue 106, November 2019

Aaminah Khan

Barrister, St John's Buildings

Clerk@stjohnsbuildings.co.uk