

## **Justifying the use of facial recognition technology in law enforcement**

20/11/2018

**Corporate Crime analysis: The Information Commissioner's Office (ICO) has issued the first Commissioner's Opinion in relation to UK regulation of the processing of personal data which takes place whenever law enforcement organisations deploy live facial recognition technology (LFR) in public spaces. Julian Hayes, partner, and Andrew Watson, legal assistant at BCL Solicitors LLP, discuss the implications of the Opinion, and emphasise the importance of establishing 'a clear and sufficient legal framework for the use of LFR in the UK' sooner rather than later.**

Original news

'Information Commissioner wants code of practice for live facial recognition', LNB News

31/10/2019 70

The ICO has released a blog post by Information Commissioner Elizabeth Denham discussing live facial recognition (LFR) technology and the role of the police in its use. She recommends that the government introduce a statutory and binding code of practice on the deployment of LFR and that 'more work should be done by a range of agencies and organisations including the police, government and developers of LFR technology to eliminate bias in the algorithms, particularly that associated with ethnicity'.

### **What in summary are the key issues identified by this Opinion?**

On 31 October 2019, the UK's data supervisory authority, the Information Commissioner (ICO) issued its first official Opinion on the use in public places of LFR by law enforcement. Intended to prompt discussion, the Opinion does not deal with the arguably less regulated private use of LFR, which the ICO is also investigating and on which it will be reporting 'in due course'.

The Opinion itself follows hot on the heels of the decision *R (on the application of Bridges) v Chief*

Constable of South Wales Police (Information Commissioner and another intervening) [2019] EWHC 2341, [2019] All ER (D) 05 (Sep) which summarises the reasoning in that case and provides a useful ‘roadmap’ for law enforcement bodies wishing to utilise LFR. However, the Opinion also raises concerns about future use including:

- the lack of a binding regulatory framework
- the legally difficult area of obtaining informed consent
- the importance of safeguarding biometric data and ensuring that any processing is undertaken
- securely and accurately
- that deployment of LFR must be both strictly necessary and proportionate
- how the efficacy of LFR is to be measured and recorded as well as addressing the problem of
- algorithmic bias
- how LFR can be used by law enforcement albeit for less obvious purposes such as identifying
- missing persons

#### **What conclusion does the ICO Opinion draw and what recommendations does it make?**

After analysing the legislative framework governing the use of LFR by UK law enforcement—in particular Part 3 of the Data Protection Act 2018 (DPA 2018)—and having acknowledged the existence of instances where LFR use will be justified, the ICO sets out the requirements which it believes must be satisfied if LFR is to be used lawfully. Key among these are that its use is ‘strictly necessary’—ie appropriately governed by policy documents, targeted at serious and violent crimes, intelligence-led and time-limited—as opposed to being used opportunistically in an unfocused way to identify perpetrators of low-level crimes such as shoplifting or those merely suspected of offences.

The ‘strict necessity’ test applies not just to the deployment of LFR but also to the composition of the ‘watchlists’ which the LFR algorithm used to find ‘matches’. In the ICO’s view, including individuals suspected or convicted of non-serious offences, or who are unlikely to be in the vicinity will be more difficult to justify. The ICO also expresses concern about the inclusion in watchlists of images which the police no longer have a legal right to retain or which have been ‘scraped’ from social media where a ‘match’ could lead to unjustified police intervention.

Most eye-catching among the ICO's recommendations is the call for the implementation of a mandatory, statutory code governing the deployment of LFR by law enforcement, based on the standards contained in the currently non-binding Surveillance Camera Code, to ensure adherence by law enforcement to consistently high standards for LFR-use, avoiding errors, and ultimately ensuring community 'buy-in' to the privacy intrusion involved in the use of the technology.

### **What impact is this Opinion likely to have?**

The ICO's power to issue Opinions derives from DPA 2018, Sch 13 and is described as 'advisory' — there is no statutory penalty for not complying with it. However, the ICO's Regulatory Action Policy suggests that one factor the data watchdog will take into account when deciding whether to take steps against those suspected of breaking information rights is whether relevant advice or guidance has been followed. Failure on the part of law enforcement to follow the ICO's Opinion is therefore likely to increase the possibility of regulatory action.

### **While law enforcement may draw some comfort from the High Court's approbatory decision**

in *Bridges*, the expressly fact-specific nature of that judgment (and the forthcoming appeal against it), mean that law enforcement will likely seek to comply with the stipulations in the Opinion when deploying LFR in future.

### **What impact has the judgment in *Bridges* had on law enforcement's use of LFR? What are the claimant's grounds for appeal?**

According to an ICO investigation into police use of LFR accompanying the Opinion, LFR use has increased rapidly in recent years. As at 31 October 2019, the Metropolitan Police Service had trialled it on ten occasions and South Wales Police had deployed it fifty times.

In the immediate aftermath of the High Court's judgment in *Bridges*, the Home Office welcomed the decision, declaring that there was a clear and sufficient legal framework for the use of LFR in the UK. The police response was more cautious. For example, in submissions to the Scottish Justice Sub-Committee on Policing, the Scottish Police Federation acknowledged the potential

intelligence-gathering benefits of the technology but urged a public education programme about it. Despite such individual expressions of caution, there was a risk that, absent the ICO's Opinion and Bridges' appeal, the High Court judgment could have been seen as a 'green light' for more widespread and possibly less controlled deployment of LFR by law enforcement.

Bridges' appeal against the High Court decision is unlikely to be heard before February/March 2020. The grounds of the appeal are not publicly available but the human rights group, Liberty (which is supporting the appeal), perhaps gave a preview when it suggested that in conducting the trials complained of by Bridges, South Wales police had breached their duty to eliminate discrimination under section 149(1) of the Equalities Act 2010 by failing to obtain information from the LFR technology provider to check the risk of bias.

This hint apart, the appeal is likely to focus on whether the interference with the appellant's rights to a private life under Article 8 of the European Convention on Human Rights was proportionate, and whether each LFR deployment was 'strictly necessary' or whether alternative less intrusive means would have sufficed (a point emphasised both in the ICO's Opinion and in a recent blog post on LFR by the influential European Data Protection Supervisor).

### **What do you see the future holding for the use of LFR by law enforcement?**

In the blog accompanying the publication of the Opinion, the Information Commissioner expressly supported police exploration of new investigative techniques, clarifying that her Opinion was not aimed at banning artificial technology from the armoury of law enforcement entirely. Rather, by calling for a statute-based and uniform approach to its use, the ICO is rightly acknowledging that, faced with ever higher public expectations, the increased use of biometrics such as LFR and gait analysis in policing methodology is inevitable. The ICO's intention is that this step into a high-tech future takes place without eroding public confidence in policing more generally.

*Interviewed by Samantha Gilbert*