ICO issues opinion on live facial recognition by law enforcement

The first Opinion under DP Act 2018 was issued by the UK's Information Commissioner on 31 October 2019. **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, it shows how high 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 the scope of the GDPR and the DP Act 2018, with police forces having to comply with Part 3 of the DP Act 2018 (law enforcement processing). 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, which is a higher bar 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.

ICO INVESTIGATION

The ICO report and Opinion follow a 17-month investigation into the use of live facial recognition by primarily South Wales Police and the Metropolitan Police Service (the Met). 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. Similar trials have been undertaken by other police forces, including the Met.

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 whilst out shopping in Cardiff City Centre. The claimant was supported in his legal action by the civil liberties group Liberty.

The ICO has raised concerns over the invasiveness of the technology for

USE OF FACIAL RECOGNITION PROGRAMMES FALLS UNDER DP LAW

In its Opinion, issued on 31 October, the ICO says that data protection law applies to the whole process of live facial recognition (LFR), from consideration about the necessity and proportionality for deployment, the compilation of watchlists, the processing of the biometric data through to the retention and deletion of that data.

"Controllers must identify a lawful basis for the use of LFR. This should be identified and appropriately applied in conjunction with other available legislative instruments such as codes of practice," the ICO says.

Based on the judgement in *R (Bridges) v The Chief Constable of South Wales* [2019] and the evidence gathered in the ICO investigation, it says that there is no basis for regulatory action.

While there is some evidence of processing good practice by both South Wales Police (SWP) and the Metropolitan Police Service (MPS), there are areas of data protection compliance where the MPS and SWP could improve practices, share lessons and reduce inconsistency.

As there is an increased risk of compliance failure and undermining public confidence, the ICO says forces and other law enforcement agencies are advised to consider the points made in the Commissioner's opinion.

some time; the Commissioner has blogged about her concerns relating to the unnecessary intrusion and potential detriment that could be caused from the use of the technology, and the ICO intervened in the *Bridges* case as an interested party, making submissions to the Court. 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. South Wales Police have subsequently continued to use the technology, although the recent use at a football match between Swansea City and Cardiff City was met with opposition from some football supporters who turned up wearing masks and with banners in protest.

Support from the public

Whilst the use of this technology is controversial, interestingly facial recognition does have relatively strong support from the general public. The ICO's investigation report revealed that there was strong public support for the use of live facial recognition for law enforcement purposes, with 82% of those asked (of a group of over 2,200 sampled) being of the view that it was acceptable for the police to use the technology. The results were also strong where it was suggested that only one person was being located, with 60% of those asked agreeing that it would be acceptable to process the faces of a crowd even if it was to locate only one person of interest, and a similarly large number (58%) thought it would be acceptable to be stopped by the police if erroneously matched. It therefore appears that, based on these results, the general public are supportive of the use of the technology in policing, although the ICO investigation report acknowledges that there is other research which has shown that the picture is not consistent across different groups in society, with lower support amongst certain groups. It would be interesting to know how public opinion would compare if asked about use of the technology in the private sector.

ICO proposes a statutory code

It could be said that we are sleepwalking even further into a surveillance society, similar to the concerns raised by the ICO in relation to the increasing use of CCTV technology over a decade ago. 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. The ICO recommends that the development of this Code be led by the government, making reference to the Surveillance Camera Code as an example. 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 framework and guidance is struggling to keep pace with the speed of technological advancement taking place. Further guidance of the use of this FRT in the private sector would also be particularly helpful, given the lack of specific available guidance in this area.

Whist the court in *Bridges* found the use of FRT to be lawful in that specific context, it has to be borne in mind that there exists a strong public interest for the use of FRT to prevent and detect crime, whereas some uses in the private sector will not necessarily justify the level of intrusion, therefore the principles of necessity and proportionality are key. In the Opinion, the Commissioner takes the view that whilst the High Court in *Bridges* found that the live facial recognition undertaken by South Wales Police was lawful, this should not be seen as a blanket authorisation to use the technology in all circumstances. Data controllers who are considering using facial recognition will also need to consider the lawful basis for processing carefully and determine the lawful basis before commencing processing. If consent is being considered as a potential basis, any power imbalance will of course be relevant – the ICO takes the view that it would be highly unlikely that consent would be a valid basis in the context of law enforcement.

> The ICO recommends that the development of this Code be led by the government, making reference to the Surveillance Camera Code as an example.

Appropriate policy document and DPIA needed

Organisations considering the introduction of this technology are advised to develop an appropriate policy document, setting out the justifications for use of the technology, in order to be able to demonstrate that its use is necessary and proportionate. In the investigation report, the ICO indicates that further guidance on appropriate policy documents is in the process of being developed.

Organisations are further advised to carry out a thorough data protection impact assessment (DPIA), which should also be well documented, to assess the impact that the processing will have on individuals and how these will be specifically addressed. The ICO's investigation report sets out a number of areas where the police DPIAs, which were reviewed as part of the investigation, could be improved with more detailed consideration about matters such as strict necessity and the proportionality considerations. One suggested area of improvement was greater involvement of the DPO, particularly in the earlier stages of the process. The ICO recommends that in respect of law enforcement agencies, DPIAs are provided to them in advance of roll out in order for early engagement with the regulator to take place.

A further recommendation of the ICO is in relation to the development of the technology's algorithms to ensure that they do not contain any technical bias, by treating certain

groups less favourably and to the extent that any technical bias may be present, that steps are taken to mitigate this factor. The ICO notes that any failure to address any such bias may have implications not only under the DP Act 2018 but also potentially for public bodies the Equality Act 2010. Fair processing information, including signage, will also be important to get right in this area, ensuring that signage is clear and that individuals are sufficiently informed of the processing being undertaken and also that data subjects are aware of how they can exercise their rights under the DP Act 2018 in relation to the processing.

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 ICO won't be the first to enforce on FRT however, as the Swedish data protection authority in August issued a GDPR penalty on this matter.[2] The case concerns a school that was piloting the use of FRT to monitor student's attendance and save teacher time in taking student register. The failings in this case relate to processing data in a more invasive manner than necessary (Article 5), processing sensitive personal data without a legal basis, consent not being valid (Article 9) and not complying with the requirements of DPIA and prior consultation with the Swedish DPA (Articles 35 and 36).

AUTHOR

Aaminah Khan is a Barrister at St John's Buildings.
Email: clerk@stjohnsbuildings.co.uk

INFORMATION

See ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf
ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf

REFERENCES

1 [2019] EWHC 2341 (Admin)
2 www.datainspektionen.se/nyheter/facial-recognition-in-school-renders-swedens-first-gdpr-fine/

ICO reminds political parties to stay within DP law

The Information Commissioner has written to the political parties in relation to the use of data in political campaigning at the general election. Elizabeth Denham wrote:

"As I set out in my letter to the political parties before the elections to the European Parliament in May 2019, the ICO's investigation into the use of data analytics for political purposes found a number of concerns relating to the use of commercial behavioural advertising techniques and the lack of transparency of profiling during recent political campaigns. The investigation identified a number of areas where action was required to improve each of the political parties' compliance with data protection law. I outlined these concerns in warning letters to political parties in July 2018."

"Following on from the warning letters, we carried out data protection audits on a number of political parties as we promised to do in our investigation report. We have been able to use some of the initial findings from these audits to improve our understanding of the data aspects of emerging campaigning techniques and current practice in political parties. We have used this knowledge to help inform our recently published draft framework code of practice for the use of personal information in political campaigning. This draft framework provides guidance on the practical application of data protection and electronic marketing laws to political campaigning practices."

She reminds the parties of data protection requirements and informs them about a specific website set up for advising political campaigners.

• *Advice to political campaigners is at ico.org.uk/for-organisations/in-your-sector/political/political-campaigning/*

Also see ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/11/information-commissioner-reminds-political-parties-they-must-comply-with-the-law-ahead-of-general-election/

'Half of organisations still not GDPR compliant'

The survey by Egress found that just over half (52%) of UK businesses are not fully GDPR compliant. A lower percentage (39.5%) of mid-sized companies reported full GDPR compliance compared with 56% of large and 51% of small companies. Also, 37% of respondents had reported an incident to the ICO in the past 12 months, with 17% having done so more than once.

Over one-third of respondents (35%) said GDPR has become less of a priority for their organisation in the last 12 months. Implementing new processes around the handling of sensitive data has been the greatest area for compliance investment in the last 12 months, said 28% of those surveyed.

The survey, which gathered views of 250 organisations of all sizes, was conducted in July 2019 by independent research organisation OnePoll on behalf of Egress.

• *See pages.egress.com/GDPR-survey-2019-uslp.html (requires providing personal details to download the free report)*
See also www.realwire.com/releases/UK-businesses-are-still-not-fully-GDPR-compliant-according-to-Egress-survey

ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Collective actions build against Google, BA, Ticketmaster, Equifax

A Group Litigation Order has been issued on British Airways with an extension to claim time, and Equifax faces representative action.
By **Laura Linkomies**.

After a slow start, we are now seeing representative action in the data protection field in the UK. The *Lloyd v Google* case has significant importance for representative action in general as the Court of Appeal recently decided that even if someone has not suffered financial or emotional damage as a result of loss or unauthorised access to their personal data, they can make a claim. Simply losing control of one's personal

Continued on p.3

Take care before you share: The ICO's draft code of practice

Private sector organisations need to pay attention too as the code recommends data sharing agreements to support accountability.
By **Rebecca Cousin** and **Cindy Knott** of Slaughter and May.

In July, the Information Commissioner's Office (ICO) published a draft Data Sharing Code of Practice ("the code"). This is a noteworthy piece of draft guidance as it will have wide-ranging application. In addition, much has changed in the data protection world since the current Data Sharing Code of Practice was published in 2011. Now is therefore a good time for organisations to review their approach to data sharing.

Continued on p.5

Future PL&B Events

- *Balancing privacy with biometric techniques used in a commercial context*, 29 January 2020, Macquarie Group, London. Speakers include Onfido on its use of biometric data and its experience of the ICO's sandbox.
- *Germany's data protection law: Trends, opportunities and conflicts,* March 2020, Covington & Burling, London
- *PL&B's 33rd Annual International Conference*, St. John's College, Cambridge 29 June to 1 July 2020.

privacylaws.com

Issue 106 **NOVEMBER 2019**

UNITED KINGDOM
report

ISSUE NO 106 **NOVEMBER 2019**

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Rebecca Cousin and Cindy Knott
Slaughter and May

Aaminah Khan
Barrister, St John's Buildings

Robert Waixel
Anglia Ruskin University

Simon Airey and Jack Thorne
Paul Hastings

Merrill Dresner
PL&B Assistant Editor

PUBLISHED BY
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com

Subscriptions: The *Privacy Laws & Business* United Kingdom Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686

ISSN 2047-1479

comment

The UK, the EU and Brexit – once again

With the general election hopefully producing an end to the Brexit deadlock one way or another, several questions remain open for the future of the UK data protection framework. As the Court of Justice of the European Union (CJEU) keeps issuing data protection decisions that are affecting practitioners' life on a daily basis, what about the future? If the UK actually leaves the EU, and is therefore no longer subject to these rulings, what will be the status of the previous rulings of the CJEU in the UK courts after exit?

If the UK leaves the EU without a Withdrawal Agreement, i.e. it has not been ratified by January 2020 and the UK has not asked/been given an extension, a no-deal Brexit would mean that organisations would need to revert to alternative arrangements for international data transfers. The DCMS is starting to prepare its own adequacy assessments – perhaps in vain in the middle of all the uncertainty (p.14).

Facial recognition has caused a stir not just in the UK but around the world. Whilst the ICO has alerted organisations to rules of fair play, France's regulator has ordered two high schools to end their facial recognition programs, and in Sweden, the DPA has imposed a fine of 200,000 Swedish Krona (£16,000) on a municipality that used facial recognition in a school (p.8)

The international conference of data protection authorities tackles these types of questions together. We were pleased to attend the conference in October in Albania, where the ICO was at centre stage as the conference Chair (p.11). We made many new contacts, as the international privacy scene is expanding rapidly with new delegates from Africa and Asia.

The decision to allow *Lloyd v Google* to proceed as a class action will have important consequences for group litigation in the UK. On 4 October, the High Court granted permission for British Airways customers to bring a group litigation order (p.1). The 2018 British Airways data breach occurred under the GDPR so we await to see whether the ICO's intention to fine the company £183,390 million will stick.

In the meantime, the ICO is consulting both on data sharing (p.1) and its aim to seize assets under the Proceeds of Crime Act 2002 (p.7).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you wish to contribute to *PL&B UK Report*? Please contact Laura Linkomies, Editor (tel: +44 (0)20 8868 9200 or email: laura.linkomies@privacylaws.com) to discuss your idea, or offer to be interviewed about your organisation's data protection/Freedom of Information work.

Join the Privacy Laws & Business community

The *PL&B United Kingdom Report*, published six times a year, covers the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.

PL&B's United Kingdom Report will help you to:

Stay informed of data protection legislative developments.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Learn about future government/ICO plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to privacy and data protection law issues and tech developments that will affect your compliance and your reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

3. Electronic Version
We will email you the PDF edition which you can also access via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments in Data Protection, Freedom of Information and related laws.

6. Back Issues
Access all *PL&B UK Report* back issues.

7. Events Documentation
Access UK events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

privacylaws.com/reports

"*PL&B* has been a data protection stalwart throughout my privacy career. Its publications continue to inform and challenge practitioners in the UK and around the world."

Simon McDougall, Executive Director – Technology and Innovation, ICO

International Report

Privacy Laws & Business also publishes *PL&B International Report*, the world's longest running international privacy laws publication, now in its 33rd year. Comprehensive global news, currently on 165+ countries, legal analysis, management guidance and corporate case studies on privacy and data protection, written by expert contributors

Read in more than 50 countries by regulators, managers, lawyers, and academics.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.