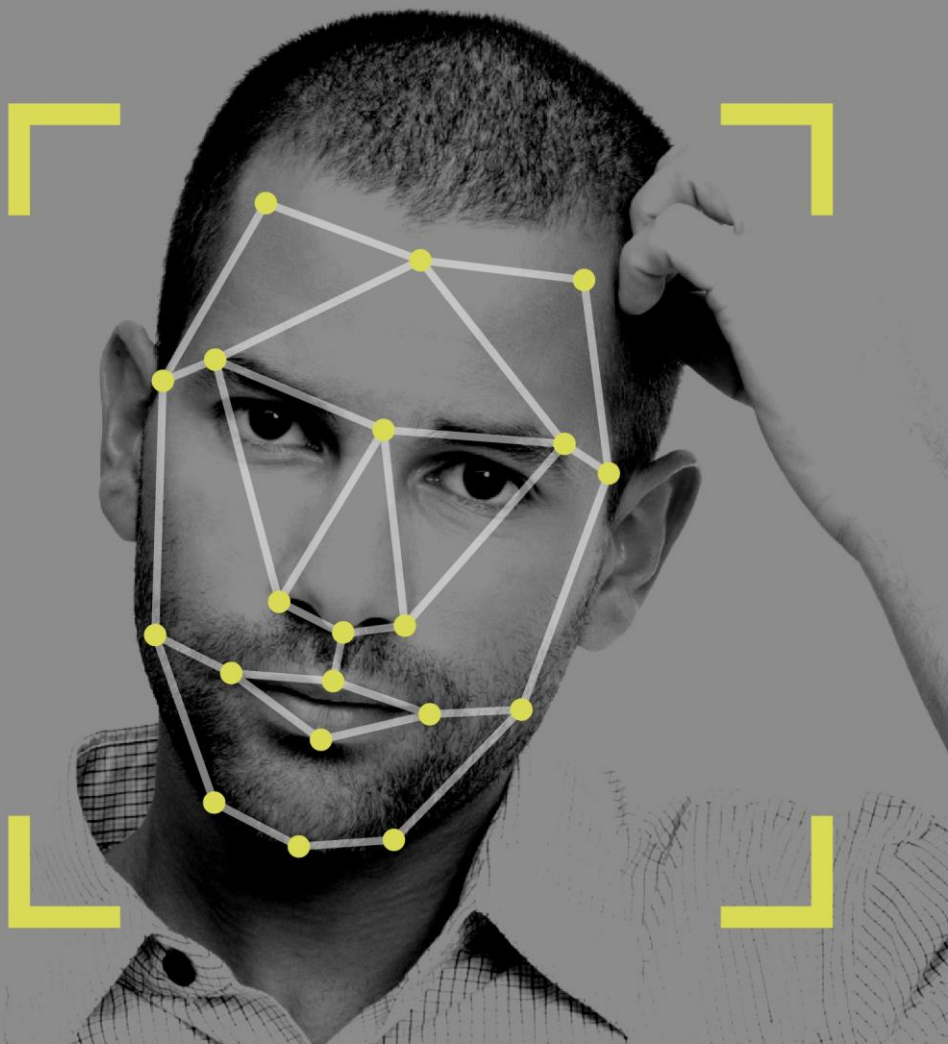
Information Commissioner's Office

ICO investigation into how the police use facial recognition technology in public places

31 October 2019



ico.
Information Commissioner's Office

Contents

Introduction

Live facial recognition (LFR) technology involves the real time automated processing of digital images containing the faces of individuals, for the purposes of identification, authentication or verification, or categorisation of those individuals. LFR is an example of a technology which processes biometric data, a particular type of data that was given specific definition within the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018).[1]

The use of LFR technology has increased rapidly in recent years, including by police forces. The Metropolitan Police Service (MPS) first deployed the technology at the Notting Hill Carnival in August 2016 and South Wales Police's (SWP) first deployment was at the UEFA Champions League Final in June 2017.

The use of LFR in public spaces by organisations, in both the public and private sectors involves the processing of personal data and requires those organisations using the technology to comply with the GDPR and the DPA 2018.

Specifically, LFR technology involves the processing of sensitive personal data, or biometric data. Biometrics is afforded an additional level of protection and requires competent authorities, law enforcement agencies, to demonstrate that the processing is strictly necessary for a law enforcement purpose and to ensure that a condition in Schedule 8 (DPA 2018) is met.

Current and future use of facial recognition technology is a regulatory priority for the Information Commissioner's Office (ICO). This is based on the following:

- scale of privacy intrusion, with the potential to affect large numbers of people, in many cases without their knowledge, as they go about their daily lives;
- the potential for facial recognition technology to enable surveillance on a mass scale, and the impact this has on individuals' human rights and information rights;

[1] http://www.legislation.gov.uk/ukpga/2018/12/section/205

- technological bias or inaccurate data that could lead to detriment, eg an individual being misidentified and potentially apprehended, thus undermining the integrity and legitimacy of the use of the technology;
- uncertainty about the effectiveness of the technology in meeting the expected law enforcement or public interest aims; and
- the potential for poor compliance to undermine public confidence in the police and trust in the technology.

The ICO also recognises the potential benefits in terms of public safety and security that appropriately governed, regulated and deployed LFR could provide. However, the deployment of the technology must be proportionate, recognising the need to strike a balance between the privacy intrusion that arises and the law enforcement purpose that needs to be met.

In view of the factors set out above, the Commissioner opened an investigation in May 2018 into the trial of LFR by SWP and the MPS[2]. These trials involved the use of LFR to locate suspects against offender databases by searching, scanning and monitoring digital images and videos. The investigation examined the forces' use of LFR and their compliance with data protection legislation.

The investigation involved significant engagement with both forces, including observations of a series of deployments in both force areas. The ICO recognises the positive engagement by both the MPS and SWP.

This report details the findings of the investigation. It would be normal practice in our investigative reports to set out a series of recommendations, based on our findings, for the data controllers to consider, in this case the MPS and SWP. However, in the case of LFR, the advice resulting from the investigation findings have a much broader relevance to the deployment or intended deployment of this technology by **any** law enforcement agency, irrespective of whether this is as part of a trial or pilot or as a routine operational tactic. For that reason, and to ensure that the data protection advice can be accessed and considered

[2] MPS have carried out 10 trials of LFR to date. SWP continue to trial LFR, having deployed over 50 times.

more easily, the Commissioner has issued for a Commissioner's opinion[3]. Law enforcement bodies reading the findings in this report should consider the advice in the supporting opinion[4].

[3] Schedule 13 DPA 2018: The Commissioner has the following investigative, corrective, authorisation and advisory powers in relation to processing of personal data to which Part 3 or 4 of this Act applies… to issue, on the Commissioner's own initiative or on request, opinions to Parliament, the government or other institutions and bodies as well as to the public on any issue related to the protection of personal data.

[4] https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf

Background

R (Bridges) v The Chief Constable of South Wales

During the ICO investigation, the use of LFR by SWP was subject to judicial review, R (Bridges) v The Chief Constable of South Wales [2019] EWHC 2341 (Admin).

The claimant submitted that SWP's use of facial recognition technology breached the right to privacy, data protection laws and anti-discrimination laws.

The Commissioner intervened in the case because of the important data protection issues arising from the complaint. In the High Court judgment[5], the relevant data protection conclusions were that:

- the use of LFR involves the processing of personal data and therefore data protection law applies;
- LFR relies on the processing of biometric data;
- the DPA 2018 is a primary piece of legislation regulating police use of LFR;
- other pieces of legislation, common law and police policies also form part of the legislative framework that regards LFR;
- the instances of SWP's use of LFR considered during the judicial review were lawful; and

The judgment did not consider that the legal framework is at present insufficient but highlighted that this will inevitably require periodic review in the future. The judgment endorsed that:

a) steps could, and perhaps should, be taken further to codify the relevant legal standards; and
b) the future development of LFR technology is likely to require periodic re-evaluation of the sufficiency of the legal regime.

Notwithstanding any appeal against the judgment, this report presents the ICO's investigation findings taking into account the decision handed down by the Court. Noting the Court's endorsement above, it is the

[5] https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf

Commissioner's view that a code should be considered at the earliest opportunity.

Views on the use of LFR

The use of the technology has had the support of government, as demonstrated by the awarding of funding from the Home Office to SWP, and through comments made by the Home Secretary. Speaking in July 2019, the then Home Secretary Sajid Javid said:

> 'I back the police in looking at technology and trialling it and...different types of facial recognition technology is being trialled especially by the Met at the moment and I think it's right they look at that'.[6]

However, significant concerns about police use of LFR have been raised. MPs in the House of Commons Science and Technology committee have called for the police use of LFR to be suspended, until further legislative framework is applied to the technology.[7]

In addition, civil society groups such as Privacy International and Big Brother Watch have both criticised police use of LFR, and Liberty has supported the Judicial Review into SWP's deployments.

Globally, concern about LFR has led to restrictions on its use. For example, San Francisco city and county agencies, including the police, are banned from using LFR. The United Nations Special Rapporteur on freedom of opinion and expression, David Kaye, has called for a moratorium of the sale and use of LFR technology. Mr Kaye's report[8] highlighted instances where LFR has been used as a means to repress particular groups, such as its use to monitor and carry out surveillance on Uighur Muslims in China.

Its use in the private sector is increasing and remains subject to a separate ICO investigation. This includes the potential for law enforcement to use private sector LFR for law enforcement purposes, including the sharing of suspects' data in combined or joint watchlists.

---

[6] https://www.bbc.co.uk/news/uk-48959380
[7] https://www.publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1970/197003
[8] https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session41/Documents/A_HRC_41_35.docx

SWP applied to the Home Office Police Transformation Fund to support their trial. According to Cardiff University's evaluation of SWP's use of LFR, the funding application provided £1.9m, with SWP committing £600,000 from their own funds[9]. It is understood by the ICO that the MPS pilots have been self-funded. The MPS has disclosed in a response to a freedom of information request that £200,000 has been spent on LFR software and hardware[10].

Both the MPS and SWP expect that LFR will improve the prevention and detection of crime. In their application for funding to the Home Office, SWP list the following policing outcomes intended from the use of LFR:

- to measurably increase potential detections;
- to see decreases in repeat offending;
- to observe a corresponding reduction in officer time spent on investigation of repeat offences;
- to increase community cohesion;
- to make savings related to reduced investigation and prosecution times;
- to support ongoing policing activity with regards to a specific problem or location;
- to assist the identification of vulnerable or at-risk individuals; and
- to protect the public at particular events.

The MPS list similar intended outcomes in their LFR operational mandate document:

- to use LFR technology to reduce and disrupt crime and to increase enforcement opportunities at selected events;
- to provide reassurance to communities that the MPS are utilising innovative and effective approaches to policing;
- to disrupt criminality and impact levels of crime;
- to increase satisfaction and confidence within London's communities by listening and responding to local concerns regarding the overt use and deployment of LFR technology at events; and

[9] https://static1.squarespace.com/static/57875c16197aea2902e3820e/t/5bdafb4403ce64828d6fbc04/1541077838619/AFR+Report+%5BDigital%5D.pdf
[10] https://www.independent.co.uk/news/uk/home-news/facial-recognition-uk-police-met-arrests-london-cost-false-positives-accuracy-a8723756.html

- to adopt a robust, proportionate and intelligence-initiated approach in engaging and pursuing individual offenders wanted within the MPS by the police and courts.

Public survey and attitudes

In January 2019, the ICO commissioned Harris Interactive to conduct market research exploring the public's awareness and perceptions about the police use of LFR in public spaces.

A total of 2,202 adults aged 18+ responded to a 10-minute online survey. Separately, 35 adults aged 18+ participated in a one-hour live chat to openly discuss the use of LFR, with certain discussion topics led by a moderator. Results of the online survey were weighted to be nationally representative of the UK by age and gender.

In summary:

- There is strong public support for the use of LFR for law enforcement purposes:
    - 82% of those surveyed indicated that it was acceptable for the police to use LFR;
    - 72% of those surveyed agreed or strongly agreed that LFR should be used on a permanent basis in areas of high crime;
    - 65% of those surveyed agreed or strongly agreed that LFR is a necessary security measure to prevent low-level crime; and
    - 60% of those surveyed agreed or strongly agreed that it is acceptable to process the faces of everyone in a crowd even if the purpose is to find a single person of interest.
- The public's support holds up even if they were to be stopped by the police as a result of LFR matching them (erroneously) to a subject of interest. 58% of those surveyed thought it was acceptable to be stopped by the police in such circumstances, while 30% thought it was unacceptable.
- However, this acceptance about LFR's use by the police and security services is balanced against concerns over privacy. Comments provided as part of qualitative research demonstrated that some only want LFR to be used where and when necessary and want to know when it is being used with the opportunity to object to images of their faces being processed and stored.

A key finding from the ICO research was that, in the main, the public are supportive of LFR use for law enforcement. However, it is important to acknowledge that support is not strong amongst all groups in society.

Research was carried out on behalf of the London Policing Ethics Panel, the (London) Mayor's Office for Policing and Crime and the University College London Institute for Global City Policing by Opinion Research Services [11]. Unlike the ICO's research, the survey was not national, but weighted to provide a representative sample of London's population. This survey again found broad support for the use of LFR for policing purposes, with 57% of all those surveyed agreeing that it was acceptable for the MPS to use LFR. But majorities of Asian (56%) and black (63%) people surveyed were opposed. Support is also lower amongst young people in London, with 55% of 16-24 and 52% of 25-39-year-olds opposed to the police use of LFR.

A national survey carried out by the Ada Lovelace Institute[12] also contains relevant data. 70% of all respondents thought that facial recognition technology should be used by the police in criminal investigations. However, support for police usage of LFR was qualified. A majority, 55%, believed that government should place limits on police use of LFR. A significant subset of people, 29%, were uncomfortable with the police using LFR due to concerns about:

- infringements on privacy;
- the normalisation of surveillance;
- a lack of opt outs or being able to consent; and
- a lack of trust in the police to use LFR ethically.

The ICO has noted the broad public support for LFR use by the police but is also mindful that support is far from universal. The public debate regarding LFR is significant, because the DPA 2018 only allows for LFR to be used by the police when it is strictly necessary for reasons of substantial public interest. Although what constitutes substantial public interest is ultimately also a matter for the courts, the views of the public help to inform the debate and is relevant in the context of policing by consent[13].

---

[11] http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/lfr_final_report_-_may_2019.pdf
[12] https://www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Public-attitudes-to-facial-recognition-technology_v.FINAL_.pdf
[13] https://www.gov.uk/government/publications/policing-by-consent/definition-of-policing-by-consent

How the police use LFR and how it works

Facial recognition technology has many applications, but during our investigation the ICO has observed police forces using it for LFR. LFR allows the police to identify individuals in real time as they pass CCTV-style cameras, referred to by SWP as 'AFR Locate'.[14]

Other uses of facial recognition technology for law enforcement purposes include the retrospective identification of individuals from older (that is, not live) CCTV footage or from still images. This use is referred to by SWP as 'AFR Identify'. Another use is similar to an 'AFR Identify' approach but uses mobile devices rather than CCTV style cameras.

Both 'AFR Identity' and mobile device examples are out of the scope of this investigation, which focusses on 'AFR Locate' type deployments by SWP and the MPS.

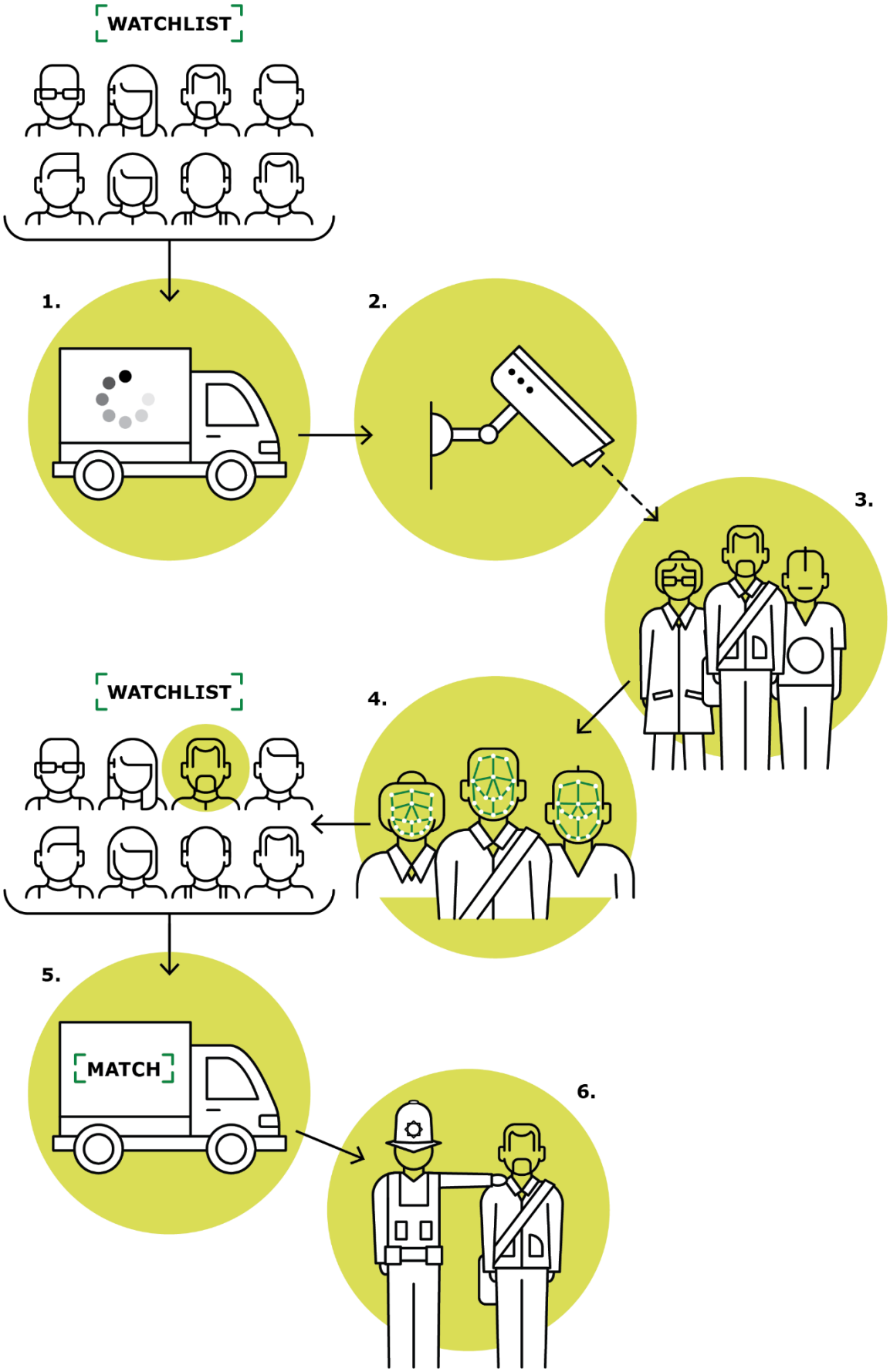
Both police forces follow a similar process for an LFR deployment. Before it commences, they compile a watchlist of subjects of interest. Generally, they use custody images to populate the list. They then decide when, where and for how long to deploy LFR.

On the ground, the police use a van as a control centre, with a Commanding Officer on board. The van contains monitors displaying footage from cameras sited nearby. As people pass by the cameras, the technology isolates facial images, converts them to a biometric template and compares these to the biometric templates of those on the watchlist.

If a potential match between the watchlist and those passing the cameras is detected, an alert is sent to officers in the van, who then advise officers on the ground if the alert is positive. The officer on the ground will then decide whether to intervene, approach or ultimately apprehend the individual. The alert may be relayed to officers on the ground by a portable device, such as a mobile phone.

[14] Whilst the ICO investigation uses the term LFR to describe facial recognition technology, SWP have used the terminology 'Automated facial recognition' (AFR). Therefore, this report will use the term LFR unless AFR has been adopted in a specific title or name by SWP such as 'AFR Locate'.

ICO observation of the police using LFR:



ICO investigation

In order to use LFR technologies lawfully, police forces must comply with data protection law, specifically Part 3 of the DPA 2018. Following the introduction of the DPA 2018, the Commissioner published a blog[15] expressing her concerns about the risks to rights and freedoms arising from the use of the technology. These concerns included unnecessary intrusion into individuals' daily lives and the potential detriment this could cause, for example unwarranted police intervention.

The Commissioner confirmed that LFR was a high priority for the ICO and ordered an investigation into its use for law enforcement purposes. The key objectives were to learn more about how it is being used by the police in the trials and to consider whether its use is compliant with data protection law.

ICO attendance at deployments

The ICO investigation involved observing LFR deployments undertaken in both London and Cardiff. In total, the ICO observed three MPS deployments and one by SWP.

Deployments observed by the ICO

Metropolitan Police Service

26 July 2018
Location: Westfield Shopping Centre
Number of individuals on watchlist: 306
Alerts generated: 1
Arrests made: 0

17 December 2018
Location: Westminster
Number of individuals on watchlist: 2,226
Alerts generated: 5
Arrests made: 2

31 January 2019
Location: Romford High Street
Number of individuals on watchlist: 2,500

[15] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/05/blog-facial-recognition-technology/

Alerts generated: 10
Arrests made: 2

South Wales Police

23 February 2019
Location: Cardiff City Centre
Number of individuals on watchlist: 830
Alerts generated: 12
Arrests made: 3

In addition to observing LFR deployments, the ICO has also gathered documentation from both forces and has carried out a data protection compliance assessment at SWP's headquarters.

We have grouped the findings of our investigation into 10 principal areas. Police forces must demonstrate compliance with data protection law in each area:

- composition of the watchlist;
- source of watchlist images;
- justification for deployment – necessity and proportionality;
- documentation;
- fair processing information provided to the public;
- retention of data;
- automated processing;
- governance and training; and
- mitigation of known bias

For each area, we have analysed the processes followed by the MPS and SWP and specific points of advice are provided regarding data protection compliance throughout the accompanying Commissioner's opinion.

Composition of the watchlist

Before any LFR deployment, police forces must compile a watchlist of individuals of interest. The technology then extracts a biometric template from the photograph, which can be compared to people walking past LFR

cameras in real time. If a match is found, an alert is generated, and officers can decide whether to intervene.

The investigation has sought to identify what considerations the police should make about the composition of a watchlist, so that:

- the use of the technology is proportionate;
- the data protection principles governing accuracy and retention of data are complied with; and
- intrusions to privacy are minimised.

The approaches of the MPS and SWP were contrasting.

In their data protection impact assessment (DPIA) for the Romford deployment, the MPS state that:

> 'Watch lists are bespoke to a given operation and are formulated to respond to the aims and objectives associated from a given operational demand, in this case wanted offenders… Each watch list is bespoke to a specific operation and encompasses intelligence which reduces the risk to the public at the given location'.

Our observation of the MPS deployment in Romford supports this intention for deployments to be bespoke for particular operations. The operational mandate for this deployment recorded the following rationale:

> 'The MPS currently (Jan 2019), have over 17000 wanted subjects. A significant number of these are wanted for violent offences, and will be subject to this pilot… As part of the pilot specific locations have been identified based on intelligence and crime patterns…identified as the geographical proximity of Romford Town Centre. This location has both footfall traffic and higher than average crime levels as identified by the MPS hotspot reporting.'

The make-up of the watchlist included those wanted for violent offences and the technology was deployed in an area where 37 violent offences were recorded in the preceding month. The aim of the deployment was also explained:

> '…details of individuals who are shown as wanted for violence related offences have been included within the watch list. It is

> intended to use this information to identify wanted persons within the principal footprint and then take appropriate actions with a view to processing them through the criminal justice systems.'

However, SWP set no such bar for the watchlist and included images of everyone on their wanted list, including those suspected of committing minor offences.

In our observation of SWP's deployment in Cardiff, during a day when a Six Nations rugby match was taking place, the watchlist compromised of 830 individuals: 280 of these individuals were on warrant for arrest; while the rest were suspects of crime.

Other than the fact that the Six Nations rugby match meant that the city would be busier than usual, there was no intelligence to suggest that the individuals on the watchlist would be in the area.

The composition of the Six Nations watchlist is akin to the composition of the watchlist considered in the Cardiff Queen Street deployment in R (Bridges) v The Chief Constable of South Wales [2019]. The court supported the actions of SWP, stating that:

> 'In fact, by including all those who were wanted on warrant there was, potentially, a considerable benefit to the public interest, without any impact on the Claimant.'

However, in the view of the Commissioner, there is a contradiction between SWP's stated intention and their practice. As set out in their DPIA:

> 'The watchlist is bespoke for each deployment, the rationale for the make-up of the watchlist is justified, proportionate and necessary with the nature of the watchlist recorded prior to each deployment.'

During her investigation, the Commissioner has been provided with no evidence that proportionality or necessity considerations were made when watchlists are constructed. SWP argues that their approach is justified, because a larger list of suspects provides a greater chance of apprehending individuals. Whilst not the sole justification, SWP also argues this provides better value for money.

The difference in approach between SWP and the MPS is clear. SWP chose to include all wanted individuals on their watchlist, whilst the MPS tailored those taking a number of factors into account including:

- the location of deployment;
- the type of crime being targeted during the deployment; and
- the nature of the crime for which suspects were of interest.

The recent judicial review hearing, R (Bridges) v The Chief Constable of South Wales [2019], considered the use of LFR by SWP. Two conclusions from the judgment in that case are worth recalling here.

Firstly, SWP have common law powers to use photographs to compile watchlists and that persons of possible interest, as well as known criminals, can legitimately be targeted as part of any watchlist.

Secondly, the DPA 2018 is the primary legislation which 'embeds key safeguards which apply to all processing of all personal data – including biometric data.'

Therefore, it is legitimate for police forces to consider any subject of interest for inclusion on a watchlist, but forces must comply with the safeguards inherent in the DPA 2018. Two safeguards are relevant here.

The first data protection principle, s35 of the DPA 2018, states that the processing of biometric data is permitted only in limited circumstances, including where the processing is 'strictly necessary'.

The third data protection principle, s37 of the DPA 2018, states that:

> '...personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed.'

Forces must ensure that watchlist data are not excessive and that the data used for watchlists are used only when strictly necessary.

The judgment also warns that, without reasonable justification for inclusion on a watchlist, an individual's human rights may also be infringed:

> 'The inclusion of any person on any watchlist and the consequent processing of that person's personal data without sufficient reason would most likely amount to an unlawful interference with their own Article 8 rights.'

In the Commissioner's view, data protection and human rights safeguards are more likely to be met when forces have carefully tailored their watchlists, minimising the number of individuals on each watchlist, and ensuring that those included are done so on the basis that it is strictly necessary to do so to meet the purposes of each deployment.

The different approach seen between SWP and the MPS adds to the risk that the public are unable to predict or foresee how the technology may be used in a given force area and a lack of consistency is therefore likely to undermine confidence in the use of the technology for law enforcement purposes.

Source of watchlist images

The ICO investigation has established that the custody images database is almost always the source of images for watchlists. The Custody Images Review (2017) uncovered serious flaws with the custody images database, in particular the retention of images.[16]

If an individual suspects that their image is retained unlawfully as part of a custody database, current procedures are that they may request that their image is deleted, but a person needs effectively to 'opt in' to do this.

There is no systematic process for the weeding of images that should have been deleted in line with police retention policies. An example of this is where images of individuals who were retained by the police, but not ultimately convicted of a crime, are kept.

The Custody Images Review explained that there are technological barriers to achieving automatic weeding of images in line with retention policies:

> 'The total numbers of images stored by the forces that participated in this Review ranged from 26,816 in the smallest of the eight

[16] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/594463/2017-02-23_Custody_Image_Review.pdf

> forces, to 7.8 million in the largest. A range of local custody systems, such as Niche, National Strategy for Police Information Systems ('NSPIS'), and Athena as well as bespoke force systems, are used to store the images… They are not generally designed to automatically weed, review or destroy images, or to differentiate between convicted and unconvicted individuals although the Athena system (currently used by seven forces) can allow images to be retained and deleted in accordance with pre-set criteria (such as the length of time retained) if this capability is enabled by individual forces.'

As further explained by Nick Hurd, then Minister for State, Home Department in a Westminster Hall debate in May 2019, the number of different systems in use further complicates matters:

> '…the fundamental issue is that, unlike the arrangements for DNA and fingerprints, there is no single national system for custody images, with a unique identifier for every record. Many records have the appropriate identifier, enabling them to be linked to arrest records. However, there are several million on the police national database that cannot be linked easily, or at all. They would have to be manually reviewed or deleted in bulk, entailing many thousands of hours of work.'

The position remains that there are potentially thousands of custody images being held with no clear basis in law or justification for their ongoing retention.

In the context of LFR, this raises concerns that unlawfully held images could be used to populate watchlists. Procedures for compiling watchlists should take this into account.

Another factor that must be considered is the use of alternative sources of images to populate watchlists. SWP state in their DPIA that custody images should be used for watchlists 'wherever possible to ensure consistency of image quality'.

It is welcome that SWP want to ensure a consistency of image quality as this will likely reduce the incidence of false positive matches, and it is reasonable to assume that lawfully retained custody images will provide this consistency. However, SWP only require custody images to be used

'wherever possible'. This suggests that other sources could be used for watchlist images.

In a DPIA, prior to their deployment in Romford, the MPS stated that watchlists should be 'constructed from relevant intelligence' and no requirements are set for image quality or consistency.

Both the DPIAs from SWP and the MPS leave enough room for a range of sources for watchlist images. This could include social media images. If such sources were to be used, it would be difficult to be assured that the images used were sufficiently accurate to avoid misidentification.

The Commissioner's 2018 investigation into the MPS's Gangs Violence Matrix found that social media was a source of intelligence. The Commissioner's findings were that:

> '...neither the Model [ie the standard operating model for officers regarding the gangs matrix] nor any other document seen by the Commissioner purports to give officers any guidance on how social media should be used, what sort of material is indicative of gang membership, what sort of material is indicative of involvement in criminal activity, or how officers should consider and approach the accuracy of such information.'

Police forces risk failures in compliance by not setting sufficiently stringent requirements for the source and accuracy of watchlist images. As per the Commissioner's investigation into the Gangs Violence Matrix, there is also a lack of guidance for officers about how to ensure the accuracy of watchlist data or which sources of watchlist images are permitted.

Justification for deployment

Demonstrating that LFR is a necessary and proportionate law enforcement tactic when considering the intrusion that arises, is key to achieving compliant processing. This investigation has noted different approaches by the MPS and SWP as to why, when and where to deploy LFR. A comparison of two of the deployments provides useful contrast to how necessity and proportionality is being considered.

MPS Romford deployment

Romford was chosen based on intelligence and violent crime patterns, as outlined in the MPS Romford operational mandate. The operational mandate stated that the use of LFR was necessary given that the location of deployment has been a borough which has experienced consistently high levels of crime and a number of offenders within the deployment footprint who were wanted by the police. Indeed, the operational mandate evidenced that there had been a recorded 37 offences with injury between 10 December 2018 and 6 January 2019, making the location within the top 10 MPS hotspots for such violent crime.

As such, this deployment was:

- informed and led by intelligence;
- based on a focussed watchlist;
- within a specific geographical area;
- had a specific objective, that is apprehending those wanted for violent offences;
- more likely to justify the intrusion, including collateral intrusion to the general public, because the objective was to detect violent crime and was focused on individuals who were known to frequent the area (ie more likely to succeed);
- led and authorised by a senior officer at the level of Commander; and
- subject to an operational mandate documenting the command structure for the deployment; operational objectives of the deployment; intelligence case for the deployment; rationale for watchlist composition and arrangements for post operation review.

SWP deployment at Six Nations

In contrast, SWP has not adopted an intelligence led approach to decide when and where to deploy LFR. Instead, and according to documents obtained during this investigation, LFR has been and continues to be deployed at large events, such as sports matches or concerts. At a briefing given to officers prior to the Six Nations

deployment, senior officers cited the basis for selection as being due to it being a busy day so there would be more likelihood of success.

SWP deployments were subject to appropriate authorisation, namely a Deputy Chief Constable acting as the Gold Commander for any deployment, which is good practice. On the other hand, the deployments were, in the Commissioner's view:

- not sufficiently led and informed by intelligence;
- based on a watchlist without specific parameters;
- insufficiently specific;
- did not have a specific objective, other than apprehending subjects of interest; and
- underpinned by underdeveloped tactical planning documents.

In the Commissioner's view, the MPS has evidenced that their deployment of LFR was necessary and proportionate more clearly than SWP.

R (Bridges) v The Chief Constable of South Wales [2019] considered the use of LFR by SWP in two deployments, on 21 December 2017 (Queen's Street) and 27 March 2018 (Motorpoint Arena). The conclusions made in the judgment regarding necessity and proportionality are generally applicable to the police use of LFR.

It was judged that SWP had used LFR proportionately because:

- deployments were for a limited time and covered a limited footprint;
- LFR was deployed for a specific purpose, the identification of wanted individuals; and
- individuals of interest to the police may have been in the area being covered by the cameras.

The Commissioner accepts that, as per the judgment, both the approach of the MPS and SWP, despite their differences, were both compliant with the DPA 2018. However, it should also be said that the differing approaches to necessity and proportionality observed between the MPS and SWP underlines the risk arising from the absence of a code of practice. The opinion provides advice on how data controllers can demonstrate that deployments are necessary and

proportionate. As with the watchlist, the different approach seen between SWP and the MPS adds to the risk that the public are unable to predict or foresee how the technology may be used in a given force area and a lack of consistency is therefore likely to undermine confidence in the use of the technology for law enforcement purposes.

Documentation

Data protection by design has always been an implicit requirement of data protection that the ICO has consistently championed. Under the GDPR and the DPA 2018, organisations have a general obligation to implement appropriate technical and organisational measures to show that they have considered and integrated the principles of data protection into processing activities.

A DPIA and Appropriate Policy Document are legal requirements for any law enforcement agency to produce prior to deployment, as set out in Part 3 of the DPA 2018. The purpose of each document is for a controller to assess the impact that any high-risk processing will have on individuals, and importantly, how **specifically** they will address these risks. They provide reassurance to the ICO and the public that the risks, including in relation to privacy intrusion, are being identified, acknowledged and mitigated at the early stages of any deployment.

These documents are key to enabling forces to demonstrate that the use of LFR is strictly necessary for policing purposes and that the requirements of data protection law are being met. An inadequate or absent DPIA would make the processing unlawful.

S64 of the DPA 2018 sets the general requirements for when a DPIA must be carried out and what it should contain[17]. A failure to carry out a lawful DPIA in accordance with s64 would make the relevant processing unlawful, contrary to the first data protection principle.

A failure to comply with s64 may be the subject of a complaint to the Commissioner under s165(2):

> 'A data subject may make a complaint to the Commissioner if the data subject considers that, in connection with personal data

[17] http://www.legislation.gov.uk/ukpga/2018/12/section/64/enacted

> relating to him or her, there is an infringement of Part 3 or 4 of this Act.'

Such a complaint may be addressed by an enforcement notice under s149(2)(c):

> 'Where the Commissioner is satisfied that a person has failed, or is failing, as described in subsection (2), (3), (4) or (5), the Commissioner may give the person a written notice (an "enforcement notice") which requires the person—
>
> a) to take steps specified in the notice, or
>
> b) to refrain from taking steps specified in the notice,
>
> ... where a controller or processor has failed, or is failing, to comply with any of the following—
>
> c) a provision of Articles 25 to 39 of the GDPR or section 64 or 65 of this Act (obligations of controllers and processors);'

The MPS and SWP shared examples of these documents with the ICO. The recognition that a DPIA is required in these circumstances is welcome, and the ICO found that these documents met the minimum requirements of the DPA 2018, but elements of each document should be improved in order to comply with the data protection principles and to show that the police are taking all reasonable steps to address the risks, specifically to members of the public that can arise.

Both the MPS and SWP updated their DPIAs to reflect any changes in the use of LFR. For the MPS this has meant updating the DPIA for each trial deployment. This included demonstrating the criteria as to why they had chosen to deploy LFR technology and use a particular 'watchlist' in that location at that time. SWP also showed good practice by demonstrating that they consulted with the public about their use of LFR at the Elvis Festival in Porthcawl.

However, the investigation found that the documentation would benefit from the following improvements:

MPS

- clearer articulation of the lawful basis for processing;
- clearer articulation about the necessity of LFR processing for policing purposes and how its use will be proportionate to the objectives of any deployment. In addition, it should explain how the use of LFR is more effective than alternative measures;
- specific assessments to the risks to the rights and freedoms of individuals and an explanation of how these risks will be mitigated;
- clear articulation of how technology bias has been eliminated and why the data controller is satisfied that this is the case;
- how the conclusions of the DPIA will be embedded into the processes governing the use of LFR;
- how and when the DPIA is to be updated;
- a record of who has approved the DPIA; and
- an explanation of the data protection officer's (DPO) involvement in the drafting of the DPIA.

SWP

- References to necessity and proportionality should be elaborated to explain why the use of LFR as a policing tactic is needed for a particular deployment ie how LFR is more effective than that of another policing tactic;
- this explanation should demonstrate why it is 'strictly necessary' for law enforcement purposes under s35(5)(a) DPA 2018, which should be justified by meeting a relevant condition in Schedule 8, as required by s35(5)(b) DPA 2018;
- the DPO should sign it in order to evidence that they have reviewed it; and
- an explanation as to how the risks of those whose biometric data is processed by the technology who are not on the watchlist are mitigated.

R (Bridges) v The Chief Constable of South Wales [2019] considered SWPs DPIA was lawful and recommended the ICO provide further guidance on Appropriate Policy documents: this work is underway.

Fair processing information provided to the public

Data subjects are often unaware that LFR technology is processing their biometric data personal data in real time. Given that a person cannot reasonably consent to having their biometric data processed through the

use of LFR technology, it has been the view of the ICO that fair processing information and signage must be overt, clear and well displayed, in accordance with s44 of the DPA 2018.

During the MPS and SWP LFR deployments, we have seen a range of interpretations of this. It was of particular concern that the MPS used an unmarked van during their Westminster deployment. However, SWP used a clearly labelled van, stating LFR technology was in use including an attributed email address.

Figure 1 – Marked van used by SWP

Figure 2- Unmarked van used by the MPS in their Westminster deployment

Figure 3 – partially marked van used by MPS in their Romford deployment

A minimum standard for meeting the requirements of the law would include clear signage that LFR is in use and telling members of the public in advance about the use of LFR.

For the public to be informed effectively, signage advertising the presence of LFR camera should be prominent. The signs should explain that:

- LFR cameras are in use;
- they process biometric data; and
- the data is being processed by the police for the stated purpose.

Vans used as control centres for LFR deployments should be marked as such.

Under s44 of the DPA 2018, forces have various duties about what information they should provide to members of the public. For example, the purposes of processing activities and how individuals can exercise their data rights. Forces must decide how to best communicate this to the public – either through signage and leaflets used during deployments, information on their website or a combination of approaches. Police forces should also make use of their website and social media platforms to inform the public about their LFR schemes in general, and of planned deployments.

Figure 4 - SWP Six Nations signage

In the deployments the ICO saw, communication to the public could have been more effective. Members of the public had little opportunity to see the signage used by the MPS in Romford, when turning out of the station and into the street (figure 5). In Cardiff, signs were small and difficult to spot in the busy

environments where signage arguably blended into the advertisements from shops and services. (SWP in Cardiff – figure 4).

Figure 5 - MSP deployed signage at the exit to Romford station, seen below the viaduct. Members of the public would already have been captured by the camera stationed on the van (to the right of the picture) before seeing the signage.

Retention of data

The fifth data protection principle requires 'that personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed'. Consequently, and also in accordance with policing codes of practice, data processed for law enforcement purposes must be subject to retention schedules, periodically reviewed and deleted when it is no longer necessary to be held. There are differences in approach to retention between the MPS and SWP.

The investigation observed that both police forces deleted the record of the LFR scanning moments after the processing, unless an alert or match was generated.

In the case of SWP, they deleted all records at the end of the deployment, including true positive matches, false positive matches and watchlist data. Therefore, they only retained it for one day.

However, the MPS retained records for 30 days, including false positive matches. The MPS justified the longer retention period because they wanted to:

- understand why the incorrect match has been made; and
- be able to respond to requests for access.

There is a distinction between the biometric data described above and general CCTV footage. SWP retained this information for 31 days, and the MPS retained for 30 days, in line with information related to false positive matches.

The DPA 2018 does not set specific retention schedules for particular types of data. However, all police forces are subject to the national retention assessment criteria and management of police information standards, which do. Any police forces using LFR must, as part of their DPIA, set their retention schedules in line with legal requirements. The retention schedules should include:

- watchlist data;
- CCTV type footage;
- positive match data; and
- false positive match data.

Automated processing

S49 of the DPA 2018 sets out an individual's right not to be subject to automated processing:

> 1. A controller may not take a significant decision based solely on automated processing unless that decision is required or authorised by law.
> 2. A decision is a "significant decision" for the purpose of this section if, in relation to a data subject, it—
>   a. produces an adverse legal effect concerning the data subject, or
>   b. significantly affects the data subject.'

This right is significant because it would be beyond the reasonable expectation of most people to be apprehended or arrested by the police based solely on a matching exercise generated by LFR technology.

The ICO does not believe that the way in which SWP and the MPS currently use LFR technology constitutes **solely** automated processing. Both the forces use LFR to identify known suspects of interest in public spaces. However, an officer always makes the decision on whether to apprehend an individual identified by the technology as matching a known suspect of interest.

As well as matching individuals, LFR software provides a percentage indicating the closeness of the match. This functionality is useful to the user because it allows for parameters to be set. For instance, a force might set the software to only generate alerts for matches of 80% or greater. This can make the generation of alerts more accurate.

It is possible that future iterations of the technology would reduce the need for human intervention to assess the likelihood of a match. Police forces need to be wary of being overly reliant on it.

The choice to intervene and apprehend individuals must remain with Officers. The technology can assist, but it must **not** take the decision, otherwise S49 of the DPA 2018 may be engaged, or infringed.

As noted elsewhere, some studies have shown that the accuracy of LFR technologies is a lower standard when used with biometric images for certain groups, particularly women or those with darker skin tones. The police need to be aware of this problem, otherwise decisions may be judged unfairly, as well as potentially unlawful.

Officers with operational responsibility for LFR deployments must receive appropriate training to ensure that decision making processes associated with LFR technology do not become automated.

Governance and training

In March 2019, the ICO made a compliance visit to SWP's headquarters to audit various processes associated with LFR because they are the leading police force in the UK for the piloting of LFR technology.

This involved interviewing key staff involved in the SWP LFR project, including the LFR project lead and the DPO. In addition, the ICO undertook a review of related policies, procedures and training documentation, and conducted telephone interviews with operational members of staff.

The site visit found governance and information risk assessment practices that demonstrated a commitment to data protection compliance, including:

- a bi-weekly stage board meeting as part of the LFR project. These meetings are attended by operational staff responsible for the day to day management of LFR and discuss:
    - data protection;

    - details of previous deployments, including their effectiveness and any lessons learned that may affect future deployments;
- updates from the stage board meetings are provided to a senior member of staff, a Deputy Chief Constable; and
- assessments are made as to whether they should deploy LFR following a command structure, with LFR viewed as a tactic amongst an array of tactics eg the use of police horses, that they could use.

The visit also presented some areas in which the ICO believes SWP could improve their compliance with data protection law which are reflected in the accompanying Commissioner's opinion but include:

- considerations about the proportionality and necessity of any LFR deployment need to be formally recorded prior to all deployments consistently;
- the DPO needs to have an active role in the assessment of LFR deployments from a data protection perspective; and
- Operational staff and their commanders need to receive specific training regrading LFR deployments and data protection compliance.

The visit and subsequent document review highlighted several recommendations that should be implemented as a priority by SWP.

Mitigation of known bias

In general there are significant concerns that LFR technology discriminates against women and BAME (black, Asian and minority ethnic) people. These concerns have been expressed in several reports, including:

- The London Policing Ethics Panel final report on LFR[18]
- Cardiff University's evaluation of South Wales Police's use of automated facial recognition[19]

[18] http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/lfr_final_report_-_may_2019.pdf
[19] https://static1.squarespace.com/static/57875c16197aea2902e3820e/t/5bdafb4403ce64828d6fbc04/1541077838619/AFR+Report+%5BDigital%5D.pdf

- Essex University's independent report on the Metropolitan Police Service's trial of LFR[20]
- The Home Office's Biometrics and Forensics Ethics Group Facial Recognition Working Group's interim report[21]
- Big Brother Watch's 'Face Off' report[22]

Each report references a 2018 study conducted by Boulamwini and Gebru[23], which found that LFR algorithms performed best for lighter skinned males and worst for darker skinned females.

Facial recognition algorithms are 'trained' by looking at a sample of test faces, but it is possible for certain technical bias to be installed into the system's decision making unintentionally. For example, the system may have a technical bias towards ethnicity if the test data does not have a balanced representation of test faces. The rate of accuracy will therefore be different for faces the system is not familiar with.

This problem was explained in an ICO blog on machine learning. The blog used an example about a loan application system, where women are under-represented in the training data used by an algorithm, but the theory is generally applicable to any training data sets that under-represent any given group.

> 'The ML [machine learning] algorithm will generate a statistical model designed to be the best fit for the data it is trained and tested on. If the male population is over-represented in the training data, the model will pay more attention to the statistical relationships that predict repayment rates for men, and less to any different statistical patterns that predict repayment rates for women[24].'

Boulamwini's study tested three commercial facial recognition algorithms designed by Microsoft, IBM and Face++[25]. The study found that it was more likely to misidentify the gender of black women than white men. The results of the study showed that gender was misidentified in:

---

[20] https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf
[21] http://www.policingthispanel.london/uploads/4/4/0/7/44076193/1pep_report-live_facial_recognition.pdf
[22] https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf
[23] http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf, p.11
[24] https://ai-auditingframework.blogspot.com/2019/06/human-bias-and-discrimination-in-ai.html
[25] It should not be read that these are the systems used by SWP or the MPS.

- up to 1 percent of lighter-skinned males in set of 385 photos;
- up to 7 percent of lighter-skinned females in a set of 296 photos;
- up to 12 percent of darker-skinned males in a set of 318 photos; and
- 35 percent of darker-skinned females in a set of 271 photos.

An implication of potential inherent bias, as highlighted by the BFEG, is that an error, bias or inaccuracy in algorithmic output results in biased decision-making on the part of human operators. This in turn could lead to an increase of people who are female and those from BAME backgrounds being wrongly stopped by the police following a 'false positive' match.

A linked concern relates to the collation of police watchlists, and where police forces choose to site LFR cameras. In his book "The Risk of Big Data Policing – surveillance, race and the future of law enforcement", Andrew Guthrie Ferguson[26] draws on two main issues in which LFR technology and its use may prejudice those from BAME backgrounds, based upon studies in the United States.

Firstly, Guthrie Ferguson points out that it is largely people from BAME backgrounds who populate police databases. He argues that if these 'racially skewed' databases of past police contacts become the justification for future police contacts, then biased data collection will distort policing operations. Similarly, the choice of where to place surveillance systems, such as LFR, can be seen as discriminatory. Guthrie Ferguson states that the choice of targeting communities of colour matters because race can distort the accuracy of technology.

The Commissioner has noted 'facial recognition systems are yet to fully resolve their potential for inherent technological bias; a bias which can see more false positive matches from certain ethnic groups[27].'

As there is a risk that the technology is biased, police forces need to mitigate against this. Such mitigations help to demonstrate that processing is fair, and that processing is lawful in terms of the DPA 2018 and the Equality Act 2010.

---

[26] Andrew Gutherie Ferguson, The rise of big data policing – Surveillance, race, and the future of law enforcement, 1st edn (New York: New York University Press, 2017)
[27] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/blog-live-facial-recognition-technology-data-protection-law-applies/

The Equality Act 2010 created the Public Sector Equality Duty, which requires public bodies to eliminate unlawful discrimination against those with protected characteristics, such as age, race or sex.

The Equality Act 2010 is regulated by the Equalities and Human Rights Commission (EHRC). The EHRC recommends that an Equality Impact Assessment (EIA) can help those delivering public services to make decisions which are fair to all.

SWP have completed an EIA and have recorded that they believe their intended use of LFR will have 'no anticipated differential impact' on any groups with protected characteristics. The reason given is that LFR relies on facial measurements, and by implication, is blind to protected characteristics such as race or sex. The ICO does not make any judgment as to the adequacy of SWP's EIA, as this is a matter for the EHRC. However, the failure to address known issues with the accuracy of LFR systems and how they are mitigated would appear to be an important omission from the EIA.

The MPS has not shared its EIA with the ICO. Their operational mandate lists legislation relevant to LFR deployments, such as the DPA 2018 and the Human Rights Act 1998. No reference is made to the Equality Act 2010. They do not state how they will uphold the Public Sector Equality Duty.

A full explanation of how police forces comply with the public sector equality duty is required. The DPA 2018 requires that any processing is lawful, so compliance with the Equality Act 2010 is also a requirement of data protection law. Current provisions from the MPS are not adequate, and SWP's EIA could be improved by exploring issues of known bias and how they are mitigated.

Conclusions and key findings

The following findings from this investigation relate specifically to SWP and the MPS' pilot deployments of LFR in public spaces and to the different approaches taken. However, the subsequent advice to the MPS and SWP about how to ensure high standards of compliance in this area has a much broader relevance to any law enforcement organisation deploying or considering the deployment of live facial recognition in public spaces. Therefore, we have issued this advice as a Commissioner's opinion. Before deploying LFR in public spaces, forces and other law enforcement agencies are advised to consider the points made in the Commissioner's opinion which has been issued under the provisions available to the Commissioner in the DPA 2018.

Key findings in this investigation

- Based on the judgement in R (Bridges) v The Chief Constable of South Wales [2019] and the evidence gathered in this investigation, there is no basis for the ICO to consider regulatory action.
- There is some evidence of processing good practice by both SWP and the MPS.
- There are areas of data protection compliance where the MPS and SWP could improve practices, share lessons and reduce inconsistency.
- There have been missed opportunities to achieve higher standards of compliance and also to improve public awareness and confidence in the technology and its use for law enforcement purposes.
- Inconsistencies in approach between SWP and the MPS are likely to be repeated in any roll out of LFR across more forces, leading to an increased risk of compliance failure and undermining public confidence.
- In particular, where this inconsistency relates to the compilation of watchlists and to individual forces' necessity and proportionality judgements, it is likely to lead to more confusion and deeper public concern and make the law less predictable and foreseeable.
- The absence of a statutory code of practice and national guidelines contributes to inconsistent practice, increases the risk of

compliance failures and undermines confidence in the use of the technology.

- Data protection legislation has specifically set a high bar for processing biometric data. The Commissioner remains of the view that the more generic the objectives and the watchlist, the more likely it is that the bar will not be met. The MPS deployments were overall more specific than that of SWP.
- Despite over 50 deployments, in the case of SWP, there is no clear articulation of what the police consider to be 'effective' or at what point the piloting phase may end. This could lead to concerns overall about effectiveness and therefore whether the high number of trials over an extended period supports or undermines the necessity and proportionality case for its use.
- Whilst there is a reduction in the number of false matches since 2017, more needs to be done to reduce technology bias and to describe the steps taken by the police to do so.
- The investigation did not identify whether staff that were involved in compiling the watchlists had guidance on how to ensure that all the images they used to compile the watchlists were accurate and lawfully retained.
- DPOs have been too peripheral in the LFR pilots and in some instances have been consulted too late in the process. This leads to concerns about forces' adherence to data protection accountability principles.
- Fair processing obligations were broadly met but with room to improve public awareness of the deployment of LFR through better positioned and clearer signage and through use of police forces' websites.