

Information Commissioner's Opinion:

The use of live facial recognition technology by law enforcement in public places

31 October 2019

Reference: 2019/01

ico.

Information Commissioner's Office

Summary

The Commissioner has previously expressed her views about the risks to the rights and freedoms of individuals arising from the disproportionate use of live facial recognition (LFR), unnecessary intrusion into individuals' daily lives and the potential detriment this could cause, eg unwarranted police intervention. In addition, the Commissioner has blogged about how data protection law applies to the processing of such biometric data.

The ICO has produced this Opinion in relation to our regulation of the processing of personal data which takes place whenever law enforcement organisations deploy facial recognition technology in public spaces. It aims to guide law enforcement through all the stages of that processing. Here are the key messages in this Opinion:

- The use of LFR involves the processing of personal data and therefore data protection law applies, whether it is for a trial or routine operational deployment.
- The processing of personal data by 'competent authorities' (s30 DPA 2018) for 'the law enforcement purposes' (s31 DPA 2018) is covered by Part 3 of the DPA 2018.
- Specifically, the use of LFR for the law enforcement purposes constitutes 'sensitive processing' (s35 (8)(b) DPA 2018) as it involves the processing of biometric data for the purpose of uniquely identifying an individual.
- Such sensitive processing relates to **all** facial images captured and analysed by the software; and must pay particular attention to the requirements of s35, s42 and s64 DPA 2018. As such, a Data Protection Impact Assessment (DPIA) and an 'appropriate policy document' must be in place.
- Sensitive processing occurs **irrespective** of whether that image yields a match to a person on a watchlist or the biometric data of unmatched persons is subsequently deleted within a short space of time.
- Data protection law applies to the whole process of 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 Commissioner intends to work with relevant authorities with a view to strengthening the legal framework by means of a statutory and binding code of practice issued by government. In the Commissioner's view, such a code would build on the standards established in the [Surveillance Camera Code](#) (issued under the Protection of Freedoms Act (POFA 2012) and sit alongside data protection legislation, but with a clear and specific focus on law enforcement use of LFR and other biometric technology. It should be developed to ensure that it can be applicable to current and future biometric technology.
- The Commissioner intends to provide more detailed guidance on what is required for police and other law enforcement agencies to comply with the obligations set out in the High Court's decision in *R (on the application of E. Bridges) v The Chief Constable of South Wales Police, The Secretary of State for the Home Department* and taking note of the Court's recommendation for her to provide guidance on what is required to meet s42 DPA 2018.

About this Opinion

What is the status of this Opinion?

The Data Protection Act 2018 (DPA 2018), specifically s116 (2) in conjunction with Schedule 13 (2)(d), allows for the Information Commissioner (the Commissioner) to issue Opinions to government, other institutions or bodies as well as the public, on any issue related to the protection of personal data.

The Commissioner can issue Opinions on her own initiative or on request. This Opinion may also form the basis of the Commissioner's approach to enforcing Part 3 and 4 DPA 2018 in this area.

The Opinion may be subject to change or may lead to future guidance and the Commissioner reserves the right to make changes or form a different view based on further findings or changes in circumstances.

Who is this Opinion for?

This Opinion is primarily for police forces or other law enforcement agencies using live facial recognition technology (LFR) in public spaces on how to comply with the provisions of the DPA 2018. It may also be a useful resource for those that have an interest in the capabilities of LFR technology and its potential applications for law enforcement. The Opinion is specifically focused on issues affecting personal data and privacy, in line with the Commissioner's regulatory responsibility. The police and other law enforcement organisations should continue to have regard to the standards and principles set out in the Surveillance Camera Code, issued under the Protection of Freedoms Act 2012 (POFA 2012).

This Opinion draws on the ICO's findings in its investigation into the trials of LFR in public spaces by South Wales Police (SWP) and the Metropolitan Police Service (MPS). Advice to those forces about the data protection issues associated with LFR has a much broader relevance and is therefore applicable to any law enforcement organisation deploying or considering deploying LFR. For that reason, the Commissioner has decided to use this advice to issue an Opinion. Law enforcement agencies should read this Opinion which is supported by the findings in the investigation report.

This Opinion also considers the judgment issued by the High Court in the case *R (on the application of E. Bridges) v The Chief Constable of South*

Wales Police, The Secretary of State for the Home Department (Interested party) (Bridges v SWP), in which the Commissioner intervened.

The Commissioner believed it was important to intervene in this judicial review, in order to assist the Court on the specific application of data protection law and associated issues arising in that case. Her submissions are reflected in this Opinion, many of which are aligned with the High Court's judgment. However, there are some areas where the High Court did not agree with the Commissioner's submissions.

The Commissioner respects and acknowledges the decision of the High Court, and her office will work with the police and other law enforcement authorities using LFR in public spaces on that basis. She will closely scrutinise the progress of any appeal. While the legislative framework underpinning the use of LFR is evolving, the Commissioner does not consider that the decision of the High Court should be seen as a blanket authorisation to use LFR in all circumstances.

The Commissioner expects that in order to give the public confidence in police use of LFR, more detail is required in Data Protection Impact Assessments (DPIAs) that controllers must ensure are in place prior to each LFR deployment. A vital point, in the Commissioner's view, is that the s35(5) requirement of 'strict necessity', which is key to the use of LFR in public spaces, requires more detailed consideration by the police and law enforcement authorities about the proportionality of the use of LFR set against the intrusion that arises; and that she would expect to see that detailed judgement in all DPIAs dealing with LFR.

The public surely expect – indeed have a right to demand – the highest standards of compliance by the police and other law enforcement authorities when processing sensitive data on a large scale and which occurs when using LFR in public areas. The Commissioner views such high standards, reflected in this Opinion, as critical to maintaining public confidence in the technology and what it is seeking to achieve. Taking full account of the High Court's judgment, the Commissioner believes that there are areas of processing personal data where the police should seek to raise the standards beyond those set out in the judgment when deploying LFR in public spaces in order to ensure public confidence in this technology.

Background

How is LFR technology used by law enforcement in public places?

The use of LFR in public spaces in both public and private sectors involves the processing of personal data under the General Data Protection Regulation and Data Protection Act 2018. This is the legislative context within which the ICO is continuing to look at the data protection issues arising from LFR processing: LFR remains an area of high priority for the ICO. This Opinion addresses the requirements of Part 3 of the DPA 2018 for processing biometric data through LFR, specifically for the 'law enforcement purposes'.

Part 3 of the DPA 2018 was designed to implement the EU Law Enforcement Directive 2016/680 (Law Enforcement Directive). As the Law Enforcement Directive has already been adopted into UK law, police forces should continue to comply with Part 3 of the DPA 2018, and follow the advice in this Opinion in the event of any form of Brexit, in line with [ICO Brexit guidance](#).

The law enforcement purposes, as defined at s31 DPA 2018, are:

'the prevention, investigation detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.'

LFR involves the real time automated processing of digital images containing the faces of individuals eg images extracted from CCTV, whose facial features are measured by LFR software to produce a biometric template of each image for the purposes of uniquely identifying, individuals. LFR is an example of technologies that process biometric data, a particular type of data that was given specific definition within the DPA 2018.

'Personal data' under s3(2) DPA 2018 means

'any information relating to an identified or identifiable living individual.'

Section 205(1) defines biometric data as

'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allows or confirms the unique identification of that individual, such as facial images or dactyloscopic (fingerprint) data, as defined at s205(1) DPA 2018'.

In order to determine a match, biometric templates are extracted from the scanned faces of individuals. In the case of LFR deployment under discussion here, these templates are cross referenced with biometric templates extracted from the scanned faces of individuals on a watchlist. The watchlist is a bespoke gallery of persons of interest created by competent authorities such as the police. After a facial match is suggested by LFR processes, human intervention is required to assess whether the match is correct and to determine the appropriate response.

What are the legal requirements under Part 3 of the DPA 2018?

Use of LFR for the purpose of identifying individuals wanted by the police is still being trialled in some areas and has not yet been rolled out more widely. However, these trials are live deployments of the technology involving real people and therefore there is no room for complacency or reduced standards. As LFR processes personal data, data protection law applies wherever and whenever it is used.

The use of LFR involves the 'sensitive processing' of biometric data within the meaning of s35(8)(b) DPA 2018 (the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual). This applies in respect of **all** facial images captured and analysed by LFR software, irrespective of whether:

- that image yields a possible match to a person on a watchlist; or
- the biometric data of unmatched persons is deleted within a short period of time.

This view is consistent with the High Court's findings in *Bridges v SWP*.

In order to comply with the first data protection principle (lawful and fair), such sensitive processing must:

- be fair;

- be 'based on law' within the meaning of s35 (1) and (2) DPA 2018, with the legal basis having to be sufficiently clear, precise and foreseeable;
- be based either:
 - on individual consent *or* for the performance of a task carried out for that law enforcement purpose by a competent authority (s35(2)(a)) and s35(4) DPA 2018; or
 - on the processing being 'strictly necessary' for the law enforcement purposes under s35(5)(a) DPA 2018, while also meeting a relevant condition in Schedule 8, as required by s35(5)(b) DPA 2018. (This would also meet the requirement of s35(2)(b)); and
- The controller must, at the time of processing, have an 'appropriate policy document' that the controller must put in place (as described in either s35(4)(b) or s35(5)(c) as well as s42 DPA 2018).

The requirement under s35(2) DPA 2018, that the processing must be 'based on law', reflects Article 10 of the Law Enforcement Directive , which provides that processing must be **authorised by Union or Member state law**.

The controller must identify a legal basis that provides a sufficiently clear, precise and foreseeable lawful justification to utilise LFR for the law enforcement purposes. This is reflected further in Recital 33 of the EU Law Enforcement Directive which contemplates that a Member State law is expected to meet these criteria:

'such a Member State law, legal basis or legislative measure should be clear and precise and its application foreseeable for those subject to it.'

The necessary legal basis may be found in more than one statute or other source of law (including in the case of LFR, the common law as to police powers).

Definitions covered by this Opinion

What does ‘lawful’ mean in this context?

Like the High Court in *Bridges v SWP*, the Commissioner accepts that the police have a power under common law to detect and prevent crime and that this power constitutes a relevant function for the purposes of condition 1 (a) of Schedule 8. In the case of populating a watchlist, the Commissioner also notes that the Police and Criminal Evidence Act (PACE)¹ may also provide the basis in law for LFR purposes.

The Commissioner’s view is that the law being relied upon for the use of LFR must have sufficient clarity and foreseeability to meet the standards required by the case law of the Court of Justice of the European Union and the European Court of Human Rights, as contemplated in [Recital 33 to the EU Law Enforcement Directive](#). In other words, could an individual reasonably expect that their image could be processed, and data captured in this way, and understand why this was happening?

The Court considered the combination of law and practice being relied upon by SWP including, amongst other things, the police common law powers, the Surveillance Camera Code (POFA 2012), PACE and the DPA 2018 and concluded that SWP were acting in accordance with the law

The Commissioner’s view is that this combination of law and practice can be made more clear, precise and foreseeable so that individuals can better understand when their biometric data may be processed by LFR. The High Court, in *Bridges v SWP*, recognised that steps could and perhaps should be taken to further codify the relevant legal standards, and that the sufficiency of the legal regime would require periodic review to ensure it keeps pace with developments in the technology. It is the view of the Commissioner that a statutory and binding code of practice, issued by government, should seek to address the specific issues arising from police use of LFR and, where possible, other new biometrics

¹ [Some sections](#) of Police and Criminal Evidence Act 1984 (PACE) only apply to England and Wales. In Northern Ireland, the relevant legislation is the Police and Criminal Evidence (Northern Ireland) Order 1989. The nearest equivalent legislation in Scotland is the Criminal Procedure (Scotland) Act 1995. The ICO has given evidence to the inquiry into the use of facial recognition technology for policing in Scotland which is being undertaken by the Scottish Parliament Justice Sub-Committee on Policing.

technologies. This would reflect developments in technology and should remain viable to deal with future technological changes in this area.

Such a code should provide greater clarity about proportionality considerations, given the privacy intrusion that arises as a result of the use of LFR, eg facial matching at scale. Without this, we are likely to continue to see inconsistency across police forces and other law enforcement organisations in terms of necessity and proportionality determinations relating to the processing of personal data. Such inconsistency, when left unchecked, will undermine public confidence in its use and lead to the law becoming less clear and predictable in the public's mind. In the event that more police forces or law enforcement organisations seek to trial the technology, or indeed opt to use it as part of standard operations, the more likely we are to see inconsistency and compliance failures. In the Commissioner's view, this code should therefore be considered by government at the earliest opportunity.

This is not just an issue about data protection so, in the Commissioner's view, development of the code should be led by government, working with the ICO, the Surveillance Camera Commissioner, the Biometrics Commissioner and the Investigatory Powers Commissioner as well as a range of other stakeholders.

In any case, law enforcement organisations will always need to articulate their lawful basis for processing in a sufficiently clear, precise and foreseeable manner to be able to justify the processing. They must do this **before** the processing starts. This assessment should be made by means of a DPIA and appropriate policy document as detailed at [s42 DPA 2018](#).

When is consent appropriate?

Recital 35 of the Law Enforcement Directive refers to the definition of consent given in the GDPR. Article 4(11) of GDPR defines consent as:

'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.'

In this light, with reference to s35(2)(a) DPA 2018, the Commissioner considers that it is highly unlikely that individuals, including those not on a watchlist, will be able to provide valid consent for the processing of their

biometric data for any of the law enforcement purposes where police use LFR in public spaces. The Commissioner therefore expects the police and other law enforcement bodies to rely on s35(2)(b), ie, that the processing is 'necessary for the performance of a task carried out by a competent authority'. This is aligned with the High Court's findings in *Bridges v SWP*. It should be underscored that this does not in itself satisfy the separate requirement for the processing to be 'based on law'.

What is an appropriate policy document?

Section 35 (5)(c) DPA 2018 requires that, at the time the processing is carried out, the controller must have an appropriate policy document in place. Section 42 specifies what this document is to contain, including:

- an explanation of how the processing complies with the relevant data protection principles; and
- An explanation of the controller's policies in relation to retention and erasure, including to give an indication of how long the data is likely to be retained.

This applies to any processing operation involving sensitive processing, including those using LFR.

In the context of *Bridges v SWP*, the Commissioner and the High Court both agreed that while the policy document in question met the basic requirements in s42 DPA 2018 to constitute an overarching appropriate policy document, it could have been more detailed. The Commissioner has taken note of the High Court's recommendation for her to provide more detailed guidance on what is required to meet the s42 obligations. This work is underway and will be published in due course.

What does 'strictly necessary' mean?

Section 35(5)(a) requires that, where a data controller engages in sensitive processing without the consent of the data subject, that processing must be 'strictly necessary for the law enforcement purpose'.

'Strictly necessary' is a high bar, but it must be reached before the sensitive processing can take place under Part 3 DPA 2018, ie, the processing must be more than merely 'necessary' for the law enforcement purpose. This recognises that:

- sensitive processing, in this case of biometric data for the purpose of uniquely identifying an individual, is taking place;

- this gives rise to higher risks to individuals' rights; and
- the processing therefore requires higher levels of protections and safeguards.

Concerns and considerations

This part of the Opinion discusses the various concerns and considerations raised by LFR, and sets out the Commissioner's views and expectations in that light.

Data protection by design and default

Privacy by design has always been an implicit requirement of data protection and the ICO has consistently championed this requirement.

Under the Law Enforcement Directive and (s57 DPA 2018), data controllers are obligated to implement appropriate technical and organisational measures. These are designed to implement the data protection principles in an effective manner and to integrate the necessary safeguards into the processing for this purpose. These obligations apply both when the controller determines the means of the processing and at the time of the processing itself – they apply throughout the lifecycle of any processing operation, from initial planning to completion.

These considerations are particularly important in relation to the use of LFR, which involves the sensitive processing of biometric data and the use of algorithms or further automated processing. These require enhanced safeguards to mitigate risks to the rights and freedoms of individuals.

If a controller is processing personal data using LFR for law enforcement purposes, they must:

- implement such measures at the earliest design stage of any proposed LFR deployment, in order to;
 - ensure that they only process personal data for a specified and necessary purpose; and
 - ensure that any LFR products or services they adopt from vendors have been designed with appropriate data protection and privacy features built in.

Data Protection Impact Assessments (DPIAs)

Section 64 DPA 2018 requires the controller to carry out a DPIA before processing if the type of processing is likely to result in a high risk to the rights and freedoms of individuals.

Because the processing of personal data using LFR qualifies as sensitive processing, the ICO expects controllers to complete DPIAs before LFR deployments, whether for trial or other operational purposes, to document both the risks posed and the safeguards necessary to mitigate them.

In this light, LFR DPIAs should:

- be completed or updated before every LFR deployment so that competent authorities are able to demonstrate that they have considered the risks to the rights and freedoms of individuals by deploying LFR;
- clearly and comprehensively explain why the use of LFR is considered strictly necessary and why less intrusive options have been ruled out;
- include a clear assessment of the likelihood that the objectives of LFR, and associated processing, will be met and how its effectiveness can be measured; and
- explain how effective mitigating measures have been implemented, including in relation to false-positive matches and algorithmic biases;
- keeping in mind that DPIAs are living documents, be subject to continual review, including to account for any changes in the circumstances of the processing or the nature of the risks.

Section 65 DPA 2018 provides that where a controller has carried out a DPIA that identifies a high risk and the controller cannot take any measures to reduce the risk, the controller must consult the ICO before the processing starts. It is unlawful for a controller to proceed in these circumstances without consulting the ICO.

The strictly necessary threshold

The data controller needs to carefully consider and document each case for processing on its merits. The Commissioner expects the controller to clearly articulate, including as part of a DPIA and an [appropriate policy document](#), why the sensitive processing of personal data through LFR, for the law enforcement purpose, meets the threshold of **strict necessity**. To meet this standard, the controller must consider the **proportionality** of the sensitive processing and the availability of viable alternatives to LFR.

The Commissioner emphasises that the purpose for which LFR is deployed is of high importance. As a general observation, there is a considerable difference between using LFR to mitigate specific serious or violent crimes and widespread deployments of LFR to identify known shoplifters. The Commissioner accepts that some minor offences may be part of more serious and organised crime, and that this may be a relevant factor, but each case must be considered on its own merits.

The Commissioner's accepts that LFR may be likelier to meet the requirements of **strict necessity** and **proportionality** where it is deployed on a targeted or smaller-scale basis and for a **narrowly defined purpose**. One example is where the police have specific intelligence showing that suspects are likely to be present at a particular location at a particular time. Another is where LFR is part of tailored security measures undertaken by a competent authority for a law enforcement purpose, such as at airports.

In other words, it is likely to be less challenging to justify sensitive processing where an LFR deployment is:

- targeted;
- intelligence led;
- time limited;

To be clear, a controller has to be able to clearly explain why the use of LFR, which is an intrusive tactic, is strictly necessary where other less intrusive options may be available.

The ICO's submissions in *Bridges v SWP* highlighted areas of data processing by SWP that were of concern to the Commissioner. In particular, the ICO considered that the SWP's justifications of strict necessity and proportionality did not satisfactorily:

- demonstrate why less intrusive means to achieve the objective had been discounted;
- ensure that the use of LFR was targeted;
- ensure the choice of location was justified by a specific cause or reasonable suspicion, or both;

The ICO therefore was of the view that SWP had not ensured that a fair balance between the strict necessity of the processing of sensitive data and the rights of individuals had been struck.

In the two deployments that were considered by the court in *Bridges v SWP*, the High Court found that SWP had met the strict necessity threshold. The High Court made that finding, the Commissioner notes, on the facts of that case. The Commissioner notes that future LFR deployment by law enforcement must still comply, in the circumstances of each case, with the requirements of the DPA 2018. The strict necessity requirement is of particular importance in ensuring that necessary safeguards are integrated in LFR technology use.

The Commissioner is concerned that, as LFR technology is used more widely, inconsistencies in determinations of strict necessity and proportionality are likely to increase. This is likely to diminish public confidence in the use of the technology and could have a negative impact on the clarity and foreseeability of the law. For these reasons, the Commissioner will be calling on government to take steps to create a clear, comprehensive statutory code of practice for LFR deployment. The clarity, consistency and certainty of a code of practice will be of assistance to police and other law enforcement agencies and to the public in equal measure.

Effectiveness

Effectiveness is a key consideration when it comes to strict necessity and proportionality. The Commissioner expects that a controller will be able to clearly explain how the technology will be effective in meeting the specified law enforcement purposes. The following paragraphs outline considerations that the Commissioner considers relevant on the question of effectiveness. The Commissioner notes that, without clear evidence of effectiveness based on a thorough and transparent evaluation process, it is difficult to see how the strict necessity threshold could be reached or how the intrusion into individuals' rights and freedoms could be considered proportionate.

As a general consideration, the Commissioner expects the police or other law enforcement agencies to apply learning from each deployment, including evidence of effectiveness in similar operational scenarios, and to carry this forward to subsequent deployments to ensure that the use of LFR on each successive occasion is truly beneficial.

In the Commissioner's view, the case for effectiveness should not be based on the ratio of matches compared to false matches, although that may be an indicator of effectiveness. Nor should effectiveness be based simply on the number of arrests enabled by LFR.

Effectiveness should be demonstrated by demonstrable benefit to the public. A possible example is where LFR results in the location and conviction of a serious offender leading, presumably, to a reduction in that individual's ability to commit serious crime.

The Commissioner will continue to look at evidence suggesting that false matches are leading to a disproportionately high number of unwarranted interventions, with associated detriment to individuals. This means that the case for deploying LFR should only be made where there is an acceptably low tolerance for, and incidence of, false matches. For this reason, a baseline figure should be clearly established in the DPIA, and grounds for confidence that this baseline can be maintained should be included, as well as a description of steps to reduce it further where possible.

From the perspective of transparency, the Commissioner believes that law enforcement agencies should ensure that sufficient information is made available to the public so that the public, and directly affected individuals, are able to understand how the law enforcement agency's measure of effectiveness informs the evolution and duration of pilot phases, as well as operational deployments. Therefore, the Commissioner believes, there needs to be greater clarity for the public on why the police believe the pilots are demonstrating effectiveness. For this reason, it is important for controllers to carefully record their evaluations of effectiveness. This is to support the high degree of transparency necessary to ensure that individuals, and the public, are confident that the decisions being made to deploy and continue to operate LFR are based on firm evidence and transparent analysis.

Watchlists

The inclusion of an image on a watchlist should meet the same high threshold for processing, ie, strict necessity. Watchlists comprising biometric images of individuals wanted or suspected of non-serious offences are, in the Commissioner's view, less likely to be able to satisfy that threshold. It will be necessary to show a justification for why the intrusion into the privacy of large numbers of individuals going about their lawful business is proportionate to the apprehension of an individual wanted for or suspected of non-serious offences. Watchlists comprising large numbers of individuals where there is no reasonable expectation that they will be in the vicinity of the LFR deployment are also likely to lead to concerns about strict necessity and proportionality and about compliance with data protection principles.

The Commissioner therefore expects watchlists to:

- be limited in size, in line with the data protection principles requiring personal data to be adequate, relevant and not excessive in relation to the intended law enforcement purpose;
- only include images that are accurate, verifiable and are lawfully held by the police at the time of use;

Furthermore, the Commissioner expects organisations using or creating watchlists to:

- delete images from the LFR system as soon as practicable where no match is suggested, in line with the data protection principles about retention and erasure;
- not use the images for a different purpose, for example for profiling or combining with other personal data; and
- be compiled by staff who have sufficient knowledge of data protection legislation to ensure they comply with the requirements of the law.

The Commissioner continues to have significant concerns about the creation of watchlists compiled using custody images that should have been deleted from police systems, in line with established retention and deletion procedures. Custody images are images of individuals who have been arrested. In many cases, these individuals are not charged with an offence or are charged but not convicted. The Commissioner calls on police to ensure they comply with the Code of Practice on the Management of Police Information 2005 and the College of Policing's Authorised Professional Practice on Retention, Review and Disposal.

Another concern is the use of watchlist images with uncertain provenance, where accuracy may be an issue (for example images sourced from social media). In both cases, a suggested LFR match may lead to an unjustified intervention and has the potential to cause unwarranted damage and distress to individuals. The same concerns extend to the sharing of watchlists between law enforcement and private sector organisations. The Commissioner will continue to assess the implications of these matters as a priority.

Notwithstanding any delay to the implementation of the National Law Enforcement Data Service, which intends to provide for the auto-deletion of custody images at the appropriate time, controllers must assure themselves that the images used are accurate and that there is a lawful basis for their retention and future use. Failure to do so is an infringement of data protection law.

Eliminating bias

The Commissioner remains concerned about the potential for inherent technical bias in the way LFR technology works. This Opinion is based on the assumption that the police have fully addressed any bias that may see gender or ethnicity unfairly represented in the processing, including the collation of watchlists. The ICO continues to develop its [internal methodology to audit algorithms](#) to, amongst other things, provide additional assurance that bias is being properly addressed by the users of these technologies and LFR technology vendors. The Commissioner will continue to monitor academic and government Opinion on the question of bias, including participation at the Law Enforcement Facial Images and New Biometrics Oversight and Advisory Board.

In order to mitigate the risk of bias within the technology against gender or ethnic groups, agencies considering deployment of LFR should:

- complete an Equality Impact Assessment with consideration to the Equality Act 2010; and
- regularly review this against legal developments (as the High Court noted in *Bridges v SWP*).

Missing persons

The Commissioner is aware of the potential for the technology to be used to identify missing persons. It will be important to see how this possible use develops in the short to medium term and we welcome the opportunity to contribute to this discussion going forward.

At present, the Commissioner's view is that the case for use of LFR in missing person cases which must meet the 'strict necessity' test depends on:

- the degree to which the missing person is considered vulnerable; and
- intelligence that the individual may be in a particular area at a particular time.

Again, the law enforcement purposes must be specified, explicit and legitimate. Accordingly, the controller should, having considered this Opinion:

- focus the deployment as far as possible in terms of geographical area, size of watchlist and duration of deployment to ensure that the processing is proportionate, and the data being processed is adequate, relevant and not excessive;
- carefully document the decisions they have made on the issues of strict necessity and proportionality identified above; and
- include clear articulation of the risks associated with the processing and the mitigations in the DPIA.

The role of the Data Protection Officer (DPO)

As required by s70 and s71 DPA 2018, it is important that the DPO assists the controller to:

- monitor internal compliance;
- inform and advise on data protection obligations;
- provide advice regarding DPIAs; and
- act as a contact point for data subjects and the ICO.

The DPO should have ongoing support from chief officers and senior board members. They should possess knowledge of data protection law that is proportionate to the type of processing carried out, taking into consideration the level of protection the personal data requires.

If the ICO is made aware of a specific concern or complaint about the processing of personal data eg through the use of LFR, we may consult with the DPO directly or seek evidence from the controller that they consulted with the DPO, or associated community, about the processing.

Conclusions

Recognise the strict necessity threshold

The Commissioner acknowledges that an appropriately governed, targeted and intelligence led deployment of LFR may meet the threshold of strict necessity for law enforcement purposes. An example is where LFR is used to locate a known terrorist suspect or violent criminal in a specific area. Such a targeted use for those kinds of significant law enforcement purposes is likelier to be proportionate to the potential intrusion into individuals' rights and freedoms.

In contrast, the blanket, opportunistic and indiscriminate processing, even for short periods, of biometric data belonging to thousands of individuals in order to identify a few minor suspects or persons of interest is much less likely to meet the high bar contemplated by the DPA 2018. In the Commissioner's Opinion, this is particularly the case if the offences are low level and there may be other less privacy intrusive options available.

Implement a code of practice

The Commissioner calls on government to introduce at the earliest opportunity a statutory binding code of practice to provide further safeguards that address the specific issues arising from the use of biometric technology such as LFR. This would further inform competent authorities within the law enforcement sector about how and when they can use LFR (and potentially other biometric modalities) in public spaces in order to comply with data protection law. It will enable increased oversight to ensure LFR use is proportionate, necessary and targeted and ensure compliance with data protection, privacy and human rights law. It could assist, for example, by providing clear boundaries in terms of proportionality and strict necessity to improve consistency. In addition, it could assist competent authorities in relation to levels of authorisation and accountability for deploying LFR. A code of practice would offer law enforcement agencies and the public alike a highly desirable level of clarity and consistency. It would also contribute to the degree of transparency necessary as the use of LFR expands.

Encourage public debate

The Commissioner encourages ongoing debate and engagement with the general public, academia and the media to highlight the use of LFR technology and improve understanding both about the technology and the

concerns about its use or future use. This will also ensure there is sufficient information in the public domain about the possible effects on the rights and freedoms of individuals.

Encourage learning within the policing sector

The Commissioner encourages those in the law enforcement sector to pool their knowledge and learning through the appropriate national forums, such as the National Police Chiefs' Council. Those within the policing community who use LFR technology, should also have sufficient training to:

- fully understand the technical capabilities of LFR;
- appreciate the potential effects on those subject to any processing of biometric data; and
- recognise the core principles of data protection legislation.

The Commissioner also strongly encourages:

- the use of consistently clear, effective and appropriate signage that takes full account of predictable foot routes;
- readily accessible fair processing information in public spaces where LFR is being deployed and on police websites; and
- clear guidance on how individuals can exercise their rights under data protection law.

Next steps

- The Commissioner will carefully consider developments in this area, including any appeal in the case of *Bridges v SWP*.
- The Commissioner will publish specific guidance on appropriate policy documents in the near future.
- The Commissioner will continue to work with key stakeholders including the Surveillance Camera Commissioner (who is responsible for the regulation of surveillance cameras under the Protection of Freedoms Act 2012), the Biometrics Commissioner (who is responsible for reviewing police use of DNA and fingerprints and has an active interest in police use of facial biometric data), and the Investigatory Powers Commissioner, (who is responsible for the regulation of targeted surveillance, which may include LFR techniques).
- The Commissioner intends to issue an Opinion on LFR use by private sector organisations, including where this use involves collaboration with the police or other law enforcement bodies.
- The Commissioner will be providing evidence to the Biometric and Forensics Ethics group's enquiry into police and private sector LFR collaboration.
- The Commissioner will continue to work as a member of the Law Enforcement Facial Images and New Biometrics Oversight and Advisory Board.

Further reading

ICO blogs:

Live facial recognition technology - data protection law applies

<https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/blog-live-facial-recognition-technology-data-protection-law-applies/>

Facial recognition technology and law enforcement

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

AI auditing framework

<https://ai-auditingframework.blogspot.com/2019/07/developing-ico-ai-auditing-framework.html>

Guidance:

ICO CCTV code of practice

<https://ico.org.uk/media/1542/cctv-code-of-practice.pdf>

External:

Surveillance Camera Commissioner's Surveillance camera code

<https://www.gov.uk/government/publications/surveillance-camera-code-of-practice>

The Biometric and Forensics Ethics Group report on LFR

<https://www.gov.uk/government/publications/Police-use-of-live-facial-recognition-technology-ethical-issues>

London Policing Ethics panel report on the Metropolitan Police Service's trial of LFR

http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/lpep_report_-_live_facial_recognition.pdf