Official Sensitive

Information Rights Unit
PO Box 57192
London
SW6 1SF
United Kingdom

Our Ref: 01/FOI/19/011430

Date: 16/12/2019

Dear Mr Ferris

Freedom of Information Request Reference No: 01/FOI/19/011430

I write in connection with your request for information which was received by the Metropolitan Police Service (MPS) on 06/09/2019. I note you seek access to the following information:

> I write to request information and records under the FOIA, regarding Metropolitan police Service's use of live, automated facial recognition technology and collaboration with external companies.
>
> 1. Has your force collaborated or cooperated with any external companies (e.g. Argent LLP, Kings Cross Central LP) in their use of live facial recognition? If yes, please provide details including the name of the companies, manner of collaboration (e.g sharing images), the time period of the collaboration, locations, any costs involved, and which uses have ceased or are continuing.
> a. If yes, did your force share images as part of the collaboration? Please provide the number of images, the source or datasets from where the images came from, a full list of purposes for which the images were shared, the legal basis on which the images were shared, and data security/management protocols around the handling of the shared data.
> b. If yes, what was the rank of the officer who authorised the collaboration? What process was followed before the collaboration was authorised?
> c. If yes, what was the protocol arranged for the event of a match alert?
> d. If yes, how many times were you alerted to a match alert? How many of those led to further police action being taken?
> e. If yes, how many true positive matches were there during the collaboration?

f. If yes, how many false positive matches were there during the collaboration?
2. Does your force have any policy guidance relating to collaboration with external companies using live facial recognition and/or the retention of images resulting from the use of live facial recognition?
a. If yes, when were the policies created? (Please provide a copy of said policies)
b. How many images captured in the course of using live facial recognition technology have been retained for storage?
3. Has your force completed a privacy impact assessment in relation to collaboration with external companies using live facial recognition technology? If so, please provide a copy.
4. Has your force scrutinised a privacy impact assessment conducted by any external companies operating live facial recognition with whom you have collaborated? If so, please describe when and provide a copy.

SEARCHES TO LOCATE INFORMATION

To locate the information relevant to your request searches were conducted within the MPS.

The searches located information relevant to your request.

DECISION

I have today decided to disclose the located information to you in full where the questions refer to held/recorded information.

In addition, and irrespective of what other information may or may not be held relating to any use of facial recognition, this request also requires the MPS to Neither Confirm Nor Deny whether it holds any further information. This is because the duty in Section 1(1)(a) of the Freedom of Information Act 2000 (the Act) does not apply, by virtue of the following exemptions;

- Section 24(2) National Security
- Section 31(3) Law Enforcement

Please see the legal annex for further information on the exemptions applied in respect of your request.

Please note this response should not be taken as an indication of whether or not the further information is held, other than what the MPS have confirmed is held within this response for your questions.

REASONS FOR DECISION

Section 24 and Section 31 are both qualified exemptions and as such there is a requirement to evidence any harm confirmation or denial that any other information is held, as well as consider the public interest.

Section 24(2) (National Security) and Section 31(3)(Law Enforcement) NCND - Harm Test in respect of confirming if additional information is held

Any disclosure under FOI is a release to the public at large. Whilst not questioning the motives behind this specific request, confirming or denying that any information relating to the any possible covert practice of facial recognition would show criminals what the capacity, tactical abilities and capabilities of the MPS are, allowing them to target specific areas of the UK to conduct/undertake their criminal/terrorist activities.

Confirming or denying the specific circumstances in which the Police Service may or may not deploy the use of facial recognition would be likely to lead to an increase of harm to covert investigations and compromise law enforcement. This would be to the detriment of providing an efficient policing service and a failure in providing a duty of care to all members of the public.

The threat from terrorism cannot be ignored. It is generally recognised that the international security landscape is increasingly complex and unpredictable. Since 2006, the UK Government has published the threat level, based upon current intelligence and that threat has remained at the second highest level ‘severe’, except for two short periods during August 2006, June and July 2007, and more recently in May and June this year following the Manchester and London terrorist attacks, when it was raised to the highest threat, ‘critical’. The UK continues to face a sustained threat from violent extremists and terrorists and the current threat level is set at ‘severe’.

It is well established that police services use covert tactics and surveillance to gain intelligence in order to counteract criminal behaviour. It has been previously documented in the media that many terrorist incidents have been thwarted due to intelligence gained by these means.

Confirming or denying whether any information is or isn’t held relating to the covert use of facial recognition technology would limit operational capabilities as criminals/terrorist would gain a greater understanding of the police’s methods and techniques, enabling offenders to take steps to counter them. It may also suggest the limitations of police capabilities in this area, which may further encourage criminal/terrorist activity by exposing potential vulnerabilities.

This detrimental effect is increased if the request is made to several different law enforcement bodies. In addition to the local criminal fraternity now being better informed, those intent on organised crime throughout the UK will be able to ‘map’ where the use of certain tactics may or may not be deployed. This can be useful information to those committing (or those intent on committing or planning) crime. It would have the

likelihood of identifying location-specific operations which would ultimately compromise police tactics, operations and future prosecutions as criminals could counteract the measures used against them.

Any information identifying the focus of policing activity could be used to the advantage of terrorists or criminal organisations. Information that undermines the operational integrity of these activities will adversely affect public safety and have a negative impact on both National Security and Law Enforcement.

Please note this response should therefore not be taken to as an indication of whether or not the further information is held, other than what the MPS have confirmed is held within this response for your questions.

Public Interest Test (Section 24(2) NCND - National Security)

Public interest considerations favouring confirming or denying whether the information is held - Section 24(2)

The confirmation or denial that the MPS holds information in relation to the covert use of facial recognition technology would provide an insight into the type of technology possibly used by the MPS for covert surveillance to protect national security.

Confirming or denial that any other information exists relevant to the request than that already provided would lead to a better informed public and the public are entitled to know how public funds are spent.

Public interest considerations favouring neither confirming nor denying whether the information is held - Section 24(2)

The MPS is charged with enforcing the law, preventing and detecting crime and protecting the communities we serve. The security of the country is of paramount importance and the MPS will not divulge whether any other information is or is not held if to do so would place the safety of an individual at risk or undermine National Security.

Whilst there is a public interest in the transparency of policing, providing assurance that the MPS is appropriately and effectively engaging with the threat from criminals, there is a very strong public interest in safeguarding both National Security and the integrity of the police in knowing that policing activity is appropriate and balanced in matters of National Security. This will only be overridden in exceptional circumstances.

To confirm or deny whether the MPS hold any additional information would allow inferences to be made about the nature and extent of national security related activities which may or may not take place. This could enable terrorist groups to take steps to avoid detection, and as such, confirmation or denial would be damaging to national security. By confirming or denying any policing arrangements of this nature would render national security measures less effective. This would lead to the compromise of

ongoing or future operations to protect the security or infra-structure on the UK and increase the risk of harm to the public.

Balancing Test (Section 24(2) NCND National Security)

The strongest reason favouring confirming or denying if information is held is taking into account there is a public interest in any possible use of this equipment.

The strongest reason favouring nether confirming nor denying whether additional information is held is to ensure law enforcement capabilities to protect national security are not undermined in any way whether additional information in this case is held or not.

On weighing up the competing interests, the MPS finds that the public interest favours neither confirming nor denying whether any additional information is held by virtue of this exemption.

Public Interest Test (Section 31(3) NCND – Law Enforcement)

Public interest considerations favouring confirming or denying whether the information is held - Section 31(3)

Confirming or denying whether any further information is held would allow the MPS to appear more open and transparent.

Public interest considerations favouring neither confirming nor denying whether the information is held - Section 31(3)

By confirming or denying whether any further information is held would mean that law enforcement tactics would be compromised which would hinder the prevention and detection of crime.

Security arrangements and law enforcement tactics are often reused and have been monitored by criminal groups, fixated individuals and terrorists. These security arrangements and tactics would need to be reviewed which would require more resources and would add to the cost to the public purse if an adverse FOIA disclosure undermined any possible operational methodology/work.

The MPS is charged with enforcing the law, preventing and detecting crime and protecting the communities we serve. The ability to protect uphold and protect law enforcement capabilities within the country is of paramount importance and the MPS will not divulge whether any other information is or is not held if to do so would place the safety of an individual at risk or undermine law enforcement capabilities due to adverse disclosure.

Whilst there is a public interest in the transparency of policing, providing assurance that the MPS is appropriately and effectively engaging with the threat from criminals, there is a very strong public interest in safeguarding law enforcement methodology and capabilities, as well as the integrity of the police in knowing that policing activity is appropriate and balanced.

Balancing Test (Section 31(3) NCND Law Enforcement)

The strongest reason favouring confirming whether additional information is held is the public interest in the use of public funds.

The strongest reason favouring neither confirming nor denying whether additional information is held is to ensure law enforcement capabilities and methodology (whether or not used in this instance) are not undermined by an adverse disclosure.

On weighing up the competing interests, the MPS finds that the public interest favours neither confirming nor denying whether any additional information is held by virtue of this exemption.

Additional Partial NCND Response - in respect of engagement of Section 24(2) (National Security) and Section 31(3) Law Enforcement)

Confirming or denying whether any other information is held in relation, for example to any possible covert use of facial recognition technology would potentially show criminals what the capacity, tactical abilities and capabilities of the MPS are, allowing them to target specific areas of the UK to conduct their criminal/terrorist activities.

Please note this response should not be taken as an indication of whether or not information in relation to the covert use of facial recognition is held or not.

DISCLOSURE

1.Has your force collaborated or cooperated with any external companies (e.g. Argent LLP, Kings Cross Central LP) in their use of live facial recognition? If yes, please provide details including the name of the companies, manner of collaboration (e.g sharing images), the time period of the collaboration, locations, any costs involved, and which uses have ceased or are continuing.

Yes – Kings Cross Estate Services.
Sharing of Images.
October 2016 – April 2017.
Kings Cross Estate
No known costs
Sharing of Images for the purpose of LFR ceased after April 2017,

a. If yes, did your force share images as part of the collaboration? Please provide the number of images, the source or datasets from where the images came from, a full list of purposes for which the images were shared, the legal basis on which the images were shared, and data security/management protocols around the handling of the shared data.

Seven images were shared under the local Information Sharing Agreement (ISA). The ISA identifies the MPS's legal basis under which the images were shared as the MPS' common law policing powers and further articulates the means by which Human Rights Act 1998 and data protection requirements were addressed.
The images were obtained from the MPS Custody Imaging System.
The purpose of the sharing was prevention or detection of crime.
The ISA provides that images were to be shared via secure email and stored at KCES on an independent server held in a secure room with restricted access. Those with access to the data were required to have been appropriately vetted.

b. If yes, what was the rank of the officer who authorised the collaboration? What process was followed before the collaboration was authorised?

Chief Inspector
Prior to any image being shared, an ISA was agreed between the parties in order to govern the image sharing.

c. If yes, what was the protocol arranged for the event of a match alert?

The dedicated MPS SPOC would be made aware to enable them to act on the intelligence as per the ISA.

d. If yes, how many times were you alerted to a match alert? How many of those led to further police action being taken?

There is no record held of whether any matches were made.

e. If yes, how many true positive matches were there during the collaboration?

There is no record held of whether any matches were made.

f. If yes, how many false positive matches were there during the collaboration?

There is no record held of whether any matches were made.

2. Does your force have any policy guidance relating to collaboration with external companies using live facial recognition and/or the retention of images resulting from the use of live facial recognition?

a. **If yes, when were the policies created? (Please provide a copy of said policies)**

Yes.
The present policy is effective as of 05/09/19. The policy provides that at present, there is to be no collaboration with any private company/body for the purposes of using a non-police LFR system.

a. **How many images captured in the course of using live facial recognition technology have been retained for storage?**

In respect of KCES no images have been retained for storage by the MPS.

No images captured during the MPS LFR trials have been retained for storage.

3. Has your force completed a privacy impact assessment in relation to collaboration with external companies using live facial recognition technology? If so, please provide a copy.

The image sharing to which this question refers is now historic. The MPS does not hold documentation which would enable it to answer this question.

4. Has your force scrutinised a privacy impact assessment conducted by any external companies operating live facial recognition with whom you have collaborated? If so, please describe when and provide a copy.

The image sharing to which this question refers is now historic. The MPS does not hold documentation which would enable it to answer this question.

Should you have any further enquiries concerning this matter, please contact me on or via email at Paul.D.O'Shea@met.police.uk, quoting the reference number above.

Yours sincerely

Paul O'Shea

LEGAL ANNEX

Section 17(1) of the Act provides:

(1) A public authority which, in relation to any request for information, is to any extent relying on a claim that any provision in part II relating to the duty to confirm or deny is relevant to the request or on a claim that information is exempt information must, within the time for complying with section 1(1), give the applicant a notice which-

(a) states the fact,
(b) specifies the exemption in question, and
(c) states (if that would not otherwise be apparent) why the exemption applies.

Section 31(3) (Law Enforcement) NCND of the Act provides:

The duty to confirm or deny does not arise if, or to the extent that, compliance with section 1(1)(a) would, or would be likely to, prejudice any of the matters mentioned in subsection (1).

Section 24(2) (National security) of the Act provides:

(2)The duty to confirm or deny does not arise if, or to the extent that, exemption from section 1(1)(a) is required for the purpose of safeguarding national security.

In complying with their statutory duty under sections 1 and 11 of the Freedom of Information Act 2000 to release the enclosed information, the Metropolitan Police Service will not breach the Copyright, Designs and Patents Act 1988. However, the rights of the copyright owner of the enclosed information will continue to be protected by law. Applications for the copyright owner's written permission to reproduce any part of the attached information should be addressed to MPS Directorate of Legal Services, 10 Lambs Conduit Street, London, WC1N 3NR.

COMPLAINT RIGHTS

Are you unhappy with how your request has been handled or do you think the decision is incorrect?

You have the right to require the Metropolitan Police Service (MPS) to review their decision.

Prior to lodging a formal complaint you are welcome to discuss the response with the case officer who dealt with your request.

Complaint

If you are dissatisfied with the handling procedures or the decision of the MPS made under the Freedom of Information Act 2000 (the Act) regarding access to information you can lodge a complaint with the MPS to have the decision reviewed.

Complaints should be made in writing, within forty (40) working days from the date of the refusal notice, and addressed to:

FOI Complaint
Information Rights Unit
PO Box 57192
London
SW6 1SF
foi@met.police.uk

In all possible circumstances the MPS will aim to respond to your complaint within 20 working days.

The Information Commissioner

After lodging a complaint with the MPS if you are still dissatisfied with the decision you may make application to the Information Commissioner for a decision on whether the request for information has been dealt with in accordance with the requirements of the Act.

For information on how to make application to the Information Commissioner please visit their website at www.ico.org.uk. Alternatively, write to or phone:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Phone: 0303 123 1113