METROPOLITAN POLICE TOTAL POLICING

Freedom of Information Request Reference No:

I note you seek access to the following information:

I write to request information and records, regarding the Metropolitan Police's use of live, automated facial recognition (AFR) technology with public surveillance cameras. Specifically, I am asking the following:

1. Does your force have any policy guidance relating to automated facial recognition and/or the storage/retention of images resulting from the use of automated facial recognition?
a. If yes, when were the policies created? (Please provide a copy of said policies)

2. Did your force complete a privacy impact assessment (PIA) before using live automated facial recognition technology?
a. If yes, on what date/s were the PIAs completed? (Please provide copies of these PIAs.)

3. Is there any policy relating to who can access the images of positive matches and false positive matches respectively?
i. If yes, when was this policy created? (Please provide a copy of said policy).
ii. If yes, who can access the images of positive and false positive matches respectively?

4. How many images captured in the course of using automated facial recognition technology have ever been retained for storage at the time this request was made?
a. How many of those images relate to:
i. Positive matches
ii. False positive matches
iii. Persons under 18 years of age (either positive or false positive matches).

5. What is the retention period for images that relate to:
a. Positive matches
b. False positive matches.

DECISION

I have today decided to disclose most of the located information to you in full with the exemption of the PIA as referred to in question 2 which is exempt by virtue of Section 22(1) (a) information Intended for Future Publication.

Section 22 - Information Intended for Future Publication

After weighing up the competing interests I have determined that the disclosure of the above information would not be in the public interest. I consider that the benefit that would result from the information being disclosed does not outweigh disclosing information relating to the Privacy Impact Assessment for the use of facial imaging.

In addition to this The Metropolitan Police can neither confirm nor deny whether any other information is held in relation to the covert use of facial recognition technology as the duty in Section 1 (1) (a) of the Freedom of Information Act 2000 does not apply by virtue of the following exemptions:

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

In considering whether or not the MPS can confirm (or deny) that this information is held, I have conducted a Prejudice Test to establish any potential harm.

Any disclosure under the Freedom of Information Act is a release to the public at large. Confirming or denying the specific circumstances in which the Police Service may or may not deploy the use of covert facial recognition would 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. 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 last 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'. To confirm or deny information is held in relation to any other information relating to the covert practise of facial recognition would show criminals what the capacity, tactile abilities of the MPS are, allowing them to target specific areas of the UK to conduct their criminal/terrorist activities.

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.
After weighing up the competing interests I have determined that the Public Interest favours the application of the neither confirm nor deny stance in respect of any other information held in relation to the covert used of facial recognition technology.

Please find below and attached information pursuant to your request above.

Q1 - Does your force have any policy guidance relating to automated facial recognition and/or the storage/retention of images resulting from the use of automated facial recognition?
a. If yes, when were the policies created? (Please provide a copy of said policies)

1. The policy the MPS is working to is contained within the original PIA. The original PIA does not include a reference to a 30 day policy. The decision was made after the initial PIA was written. It has been incorporated into the review of the PIA presently awaiting review and sign off. It is still due to be published in the second quarter of 2018.

Q2 - Did your force complete a privacy impact assessment (PIA) before using live automated facial recognition technology?
a. If yes, on what date/s were the PIAs completed? (Please provide copies of these PIAs.)

2. Yes, the PIA was written in April 2017.

Q3 - Is there any policy relating to who can access the images of positive matches and false positive matches respectively?
i. If yes, when was this policy created? (Please provide a copy of said policy).
ii. If yes, who can access the images of positive and false positive matches respectively?

3. Access to retained images has been incorporated into the review of the PIA. Only MPS personnel (Officers & Staff) who are assigned to the live FR deployment are authorised to access the recorded footage and alert images generated by the FR system.

Q4 - How many images captured in the course of using automated facial recognition technology have ever been retained for storage at the time this request was made?
a. How many of those images relate to:
i. Positive matches
ii. False positive matches
iii. Persons under 18 years of age (either positive or false positive matches).

A total of 104 alerts have been generated by the FR system.

2 of these are confirmed positive identifications

102 of these are incorrect system alerts. Please note that we do not consider these as false positive matches because additional checks and balances are in place to confirm identification following system alerts.

The age of the subject is not recorded

Q5 - What is the retention period for images that relate to:
a. Positive matches
b. False positive matches.

5. 30 days

I would like to take this opportunity to thank you for your interest in the Metropolitan Police Service.

Information Rights Unit