Dear Ms Carlo

**Freedom of Information Request Reference No: 2018030000340**

I write in connection with your request for information which was received by the Metropolitan Police Service (MPS) on 07/03/2018. I apologise for the delay in getting this response to you. I note you seek access to the following information:

I write to request information and records under the FOIA, 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.

**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 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.

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

Confirming or denying that any other information is held in relation to the 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 to as an indication of whether or not information in relation to the covert used of facial recognition information is held.

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

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

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.

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

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.

4. 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

5. 30 days

Should you have any further enquiries concerning this matter, please contact me on 0207 230 63147 or via email at Jennifer.Powell@met.police.uk , quoting the

reference number above.

Yours sincerely

**Jennifer Powell**
**Freedom of Information Manager**

**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 24(2) of the Act provides:**
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.

**Section 31(3) 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).

**Evidence of Harm Section 24 and Section 31**
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.

**Public interest considerations favouring confirming or denying whether the information is held - Section 24**
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 used by the force for covert surveillance.

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

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.

**Public interest considerations favouring confirming nor denying whether the information is held - Section 31**

To confirm or deny information is held would increase public knowledge in the type of technology used by the police. It will also allow for a greater understanding as to where force funds are being spent.

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

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 are or are not deployed. This can be useful information to those committing crimes. 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.

**Balance test**

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.

**Section 22 of the Act provides:**
(1) Information is exempt information if-
(a) the information is held by the public authority with a view to its publication, by the authority or any other person, at some future date (whether determined or not),
(b) the information was already held with a view to such publication at the time when the request for information was made, and
(c) it is reasonable in all the circumstances that the information should be withheld from disclosure until the date referred to in paragraph (a).

**Public interest considerations favouring disclosure - Section 22**
When information is released under the Act, it is disclosed to the world. It is only right that the MPS is seen as being open and transparent in the way that it operates and there is a genuine public interest with regards to the Privacy impact Assessment for the use of facial imaging to arrest wanted offenders. In addition, the disclosure of the requested information would enhance public knowledge in this subject matter and disclosure of the requested information is likely to support better informed public awareness and debate regarding the subject of facial recognition.

**Public interest considerations favouring non-disclosure** - **Section 22**
Consideration of the information is required prior to its public release. The spending of additional time and public funds may be wasteful if this information was to be extracted and redacted specifically for this request. The MPS have confirmed that in order to be fully transparent with the use and operational application of this equipment the intention is to publish a redacted version of the Privacy Impact Assessment in the near future.

**Balance Test**
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 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

**Find us at:**

**Facebook: https://m.facebook.com/metpoliceuk**

**Twitter: @metpoliceuk**