

Dear Ms Krueckeberg

**Freedom of Information Request Reference No: 2018030000548**

I write in connection with your request for information which was received by the Metropolitan Police Service (MPS) on 15/03/2018. I apologise for the delay in getting this information to you. I note you seek access to the following information:

I write to request information and records under the FOIA, regarding the deployment of automated facial recognition technology by the Metropolitan Police at the Cenotaph on Remembrance Sunday 2017 and Notting Hill Carnival in 2016 and 2017.

Specifically, I am asking the following:

- 1.What was the operational justification for the use of automated facial recognition by the Metropolitan Police at Notting Hill Carnival 2016 and Notting Hill Carnival 2017?
- 2.Does the Metropolitan Police have statistics on the ethnicities of those on the automated facial recognition watchlist at Notting Hill Carnival 2016 and Notting Hill Carnival 2017. If yes, please provide these statistics?
- 3.Has the automated facial recognition software used by your force been tested to ensure there is no gender or racial bias? If yes, please provide the dates/time frames of testing.
- 4.What was the operational justification for the use of automated facial recognition on Remembrance Sunday 2017 using a database of individuals not wanted by the police for any offence?
- 5.Does your force have statistics on the ethnicities of those on the automated facial recognition watchlist used at Remembrance Sunday 2017?
6. From where was the image database of fixated individuals used on Remembrance Sunday 2017 sourced? .

**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 some of the requested information. Some data has been withheld as it is exempt from disclosure and therefore this response serves as a Refusal Notice under Section 17 of the Freedom of Information Act 2000 (the Act). Please see the legal annex for further information on the exemptions applied in respect of your request.

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

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 find below information we are able to release pursuant to your request above.

1. To ensure police services reduce public risk & maintain public safety the MPS aims to reduce the amount of offenders 'at large'. The MPS are obligated to actively pursue individuals who are wanted for arrest by the police or wanted on arrest warrants issued by the Courts, which are circulated on PNC. A key factor to reducing the amount of wanted offenders is to explore technical solutions to locating and arresting wanted offenders using minimal resources.

2. No

3. The National Institute of Standards & Technology run large scale independent tests of facial recognition systems. They have stated that 1:N systems are largely untested for demographic effects.

[https://www.nist.gov/sites/default/files/documents/2017/11/20/grother\\_11\\_02\\_bias.pdf](https://www.nist.gov/sites/default/files/documents/2017/11/20/grother_11_02_bias.pdf)

4. With regards to Remembrance Sunday 2017 it was deemed proportionate and necessary to use facial recognition to identify persons whose previous behaviour at similar events has compromised the security plan, or who by their previous behaviour could be easily expected to compromise the security in place for the National Service of Remembrance.

5. No

6. . All images were obtained from legitimate police sources, these being custody imaging or taken by police/Fixated Threat Assessment Centre - usually outside a protected site or during a previous event.

There were no images used for this deployment that were taken without the subjects knowledge.

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.

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](http://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

**Consider our environment - please do not print this email unless absolutely necessary.**

NOTICE - This email and any attachments may be confidential, subject to copyright and/or legal privilege and are intended solely for the use of the intended recipient. If you have received this email in error, please notify the sender and delete it from your system. To avoid incurring legal liabilities, you must not distribute or copy the information in this email without the permission of the sender. MPS communication systems are monitored to the extent permitted by law. Consequently, any email and/or attachments may be read by monitoring staff. Only specified personnel are authorised to conclude any binding agreement on behalf of the MPS by email. The MPS accepts no responsibility for unauthorised agreements reached with other employees or agents. The security of this email and any attachments cannot be guaranteed. Email messages are routinely scanned but malicious software infection and corruption of content can still occur during transmission over the Internet. Any views or opinions expressed in this communication are solely those of the author and do not necessarily represent those of the Metropolitan Police Service (MPS).

**Find us at:**

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

**Twitter:** @metpoliceuk