Freedom of Information Request Reference No:

I note you seek access to the following information:

1. Are the Met currently trialling or using, or have the force ever trialled or used, any form of predictive policing programme?

If so, please provide the following information:

2. The name given to this predictive policing programme
3. When the programme was first used and whether it is still in use/when use ceased
4. How this predictive policing programme works, specifically:
   4.1. What data is used by the programme
   4.2. Whether it operates using algorithms or artificial intelligence
   4.3. What human interaction or oversight is required
5. The specific hardware and/or software used to build this predictive policing programme
6. Any guidance documents provided in relation to the use of this predictive policing programme
7. Any testing or research conducted in relation to this predictive policing programme
   7.1. In particular, any examination as to potential bias within the software and the exacerbation of pre-existing inequalities
8. The Privacy Impact Assessment conducted in relation to this predictive policing programme

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).

6. Any guidance documents provided in relation to the use of this predictive policing programme
The information requested for question 6 is exempt by virtue of the following exemption:

**Section 31(a)(b) - Law Enforcement**

Before I explain the reasons for the decisions I have made in relation to your request, I thought that it would be helpful if I outline the parameters set out by the Freedom of Information Act 2000 (the Act) within which a request for information can be answered.

The Act creates a statutory right of access to information held by public authorities. A public authority in receipt of a request must, if permitted, confirm if the requested information is held by that public authority and, if so, then communicate that material to the applicant. The right of access to information is not without exception and is subject to a number of exemptions, which are designed to enable public authorities to withhold information that is not suitable for release. Importantly, the Act is designed to place material into the public domain, that is, once access to information is granted to one person under the Act, it is then considered public information and must be communicated to any individual should a request be received.

Section 1 of the Act places two duties on public authorities. Unless exemptions apply, the first duty at Section 1(1)(a) is to confirm or deny whether the information specified in a request is held.

The second duty at Section 1(1)(b) is to disclose information that has been confirmed as being held. Where exemptions are relied upon Section 17 of the Act requires that we provide the applicant with a notice which: a) states that fact, b) specifies the exemption(s) in question and c) state (if that would not otherwise be apparent) why the exemption applies.

Having located and considered information relevant to your request, I am afraid that I am not required by statute to release the information requested in full. This email serves as a Partial Refusal Notice under Section 17 of the Act.

**Section 31 Law Enforcement**

In order for the exemption provided under Section 31(1) to be engaged in this case, the MPS must show that disclosure under the Act would, or would be likely to, prejudice law enforcement functions, namely Section 31(1)(a) the prevention and detection of crime and Section 31(1)(b) the apprehension or prosecution of offenders.
In this case, this exemption has been applied as disclosure of the information requested would prejudice areas within law enforcement such as the detection of crime and the apprehension or prosecution of offenders.

The MPS is charged with enforcing the law and preventing and detecting crime. Any information released under the Act which reveals information related to the gathering of intelligence and police strategies and tactics would prejudice the prevention and detection of crime and the apprehension or prosecution of offenders.

The disclosure of this information to the public by the MPS would undermine the MPS’s ability to properly police on a day to day basis. Release of the specific details of operational policing guidance for our crime mapping program used by the MPS would allow those wishing to disrupt day to day policing to use the information to assist in evading detection should they be planning any unlawful acts.

After weighing up the competing interests I have determined that the disclosure of these emails in full would not be in the public interest.

DISCLOSURE

Q1 - Are the Met currently trialling or using, or have the force ever trialled or used, any form of predictive policing programme?

The Met are not currently trialling any predictive policing software. We did conduct a number of small trials 3 years ago with PredPol, Azavea and Palantir Predictive Crime Mapping products. Concurrently, we utilised a system developed within the Met. At the end of the trial the decision was taken that the cost of implementing the commercial products was too great.

Q2 - The name given to this predictive policing programme

There was no programme to implement this.

Q3 - When the programme was first used and whether it is still in use / when use ceased

The external trails ran for 12 months (May 2014 - April 2015) the internal process is still in use.
Q4 - How this predictive policing programme works, specifically:

The internal product we currently use looks at the location of previous offences, the proximity to other similar offences and to the time that has elapsed since an offence was committed.

Q4.1 - What data is used by the programme

The internal product we currently use uses reported crime data, both the location and date/time of the offences.

Q4.2 - Whether it operates using algorithms or artificial intelligence

The internal product uses a simple algorithm looking at time and distance.

Q4.3 - What human interaction or oversight is required

The internal product runs automatically but the response to the output is subject to local interpretation by police officers where tasked to action this information. It is used to inform preventive policing, such as hotspot patrolling.

Q5 - The specific hardware and/or software used to build this predictive policing programme

The internal product uses a commercial ETL Tool (Extract Transfer & Load) to build the predictive crime areas and a similar tool to generate the output. These tools run on a standard Windows Workstation.

Q7 - Any testing or research conducted in relation to this predictive policing programme.

There was no Programme of activity to test.

Q7.1 - In particular, any examination as to potential bias within the software and the exacerbation of pre-existing inequalities
With the internal product there is no information used that contains any details other than the location of the offence and the date and time the offence was committed.

**Q8 - The Privacy Impact Assessment conducted in relation to this predictive policing programme**

A DPIA was not completed for this tool as it was introduced before the new data legislation.

I would like to take this opportunity to thank you for your interest in the MPS.

**Information Rights Unit**