17 January 2020

Freedom of Information Request - Reference No: 20193384

REQUEST

I would like to know the following under the Freedom of Information act relating to your force's use of facial recognition technology.

- When did your police force introduce facial recognition technology? Please provide a month and year.
- How does your police force use facial recognition technology? Please confirm if it is used for any of the following use cases and provide information of any additional use cases: event management, riot policing, to monitor train stations, in airports, to monitor public spaces (please confirm the type of public spaces it is installed in – i.e. shopping mall), body-worn cameras, etc.
- How much money was invested in facial recognition technology over the previous five years. Please share the figure broken down by each year for 2015, 2016, 2017, 2018 and 2019
- Does your police force plan to use facial recognition technology in 2020?
- If your police force plans to use facial recognition technology in 2020, how much money is expected to be spent on the technology and what percentage of the force's technology budget does it represent?
- If your police force does not use facial recognition technology, by the end of which year do you plan to introduce it (i.e. by end of year 2020, 2021, 2022, 2023, 2024, 2025 etc.)?

CLARIFICATION

You were signposted to the following web links:

https://www.southyorkshire.police.uk/find-out/accessing-information/request-information-under-the-freedom-of-information-act/facial-recognition-ref-20191992/

https://www.southyorkshire.police.uk/find-out/accessing-information/request-information-under-the-freedom-of-information-act/facial-recognition-software-ref-20181495/

https://www.southyorkshire.police.uk/find-out/accessing-information/request-information-under-the-freedom-of-information-act/facial-images-ref-20180945/

https://www.southyorkshire.police.uk/find-out/accessing-information/request-information-under-the-freedom-of-information-act/facial-recognition-ref-20171723/

RESPONSE

Section 17 of the Freedom of Information Act 2000 requires South Yorkshire Police, when refusing to provide such information (because the information is exempt), to provide you the applicant with a notice which:

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

The exemption applicable to your request falls under Section 21.

Section 21 *'Information which is reasonably accessible to the applicant'.*

Similar information has recently been requested via other FOI requests, the responses to which have been provided to you via links to our website in our Clarification above; the web link below will take you to the most pertinent:

https://www.southyorkshire.police.uk/find-out/accessing-information/request-information-under-the-freedom-of-information-act/facial-recognition-software-ref-20181495/

To provide further clarity, our formal response to your request above is 'no information held'.

South Yorkshire Police can neither confirm nor deny that we hold any further information relevant to this request by virtue of the following exemptions:

Section 24(2) National Security

Section 24 and Section 31 are both qualified exemptions and as such there is a requirement to evidence any harm that confirming or denying that any other information is held, in addition to considering the public interest.

Harm in confirming that Information is held
Any disclosure under FOI is a release to the public at large, confirming or denying that any other information relating to the covert practise of facial recognition would show criminals what the capacity, tactical abilities and capabilities of the force are, allowing them to target specific areas of the UK to conduct 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 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 is currently categorised as 'substantial', see below link:

https://www.mi5.gov.uk/threat-levels

The UK continues to face a sustained threat from violent extremists and terrorists.

It is well established that police forces 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 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.

Public Interest Test

Section 24 - Factors favouring confirming or denying that any other information is held

Confirming or denying that any other information exists relevant to the request would lead to a better informed public and the public are entitled to know how public funds are spent on and what security measures are in place.

Section 24 - Factors against confirmation or denying that any other information is held

Confirming or denying whether any information is or isn't held relating to the use of this type of 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.

Section 31 – Factors favouring confirming or denying that any other information is held

By confirming or denying whether any relevant information is held, would allow the public to gain a greater understanding of where public funds are being spent. Better public awareness may lead to more information from the public.

Section 31 - Factors against confirmation or denying that any other information is held

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. This may 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

The Police Service 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 Police Service 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.

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 technology may or may not be deployed. This can be use 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.
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.

It is therefore my opinion that for these issues the balancing test for confirming or not that any further information is held, is not made out.