



FREEDOM OF INFORMATION REQUEST



Request Number: F-2018-02564

Keyword: Operational Policing

Subject: Facial Recognition

Request and Answer:

Your request for information has now been considered. In respect of Section 1(1)(a) of the Act I can confirm that the Police Service of Northern Ireland does hold information to which your request relates. The decision has been taken to disclose the following.

I write to request information and records under the FOIA, regarding your police force's use of live, automated facial recognition technology.

Request 1

Has your police force discussed using live facial recognition with external companies, or other police forces? If so, please provide details, including of any demonstrations.

Answer

PSNI intends to include the use of facial recognition technology within its Biometric programme.

There is no current project or date set yet for initiation of a project.

PSNI is engaged with the Biometric Modalities Oversight and Advisory Board that is chaired by a National Police Chiefs Council (NPCC) member and brings together police forces and other interested bodies across the UK.

Request 2

Has your police force used live facial recognition? If so, please provide details including the time period of use, locations, and which uses have ceased or are continuing.

Request 3

Has your force collaborated with any external companies in the course of their use of live facial recognition? If so, please provide details including the time period of use, locations, any costs involved, and which uses have ceased or are continuing.

Request 3A

If the answer to 3 is yes, what was the protocol arranged for the event of a match alert?

Request 3B

If the answer to 3 is yes, how many times was your force informed of a match alert? How many of

those led to further police action being taken?

Request 4

How many true positive matches were there during your force's use, or engagement with external use, of live facial recognition?

Request 5

How many false positive matches were there during your force's use, or engagement with external use, of live facial recognition?

Request 6

Does your force have any policy guidance relating to live facial recognition and/or the retention of images resulting from the use of live facial recognition?

Request 6A

If yes, when were the policies created? (Please provide a copy of said policies)

Request 6B

How many images captured in the course of using automated facial recognition technology have been retained for storage?

Request 7

Has your force completed a privacy impact assessment in relation to live facial recognition technology? If so, please provide a copy.

Request 8

Has your force scrutinised a privacy impact assessment conducted by any external companies operating live facial recognition with whom you have collaborated? If so, please describe when and provide a copy.

Request 9

Has your force shared facial images with external companies for the purposes of live facial recognition? If so please detail:

- a. which companies the images were shared with,
- b. the number of images shared,
- c. from which datasets the images were drawn,
- d. a full list of purposes for which the images were shared,
- e. the legal basis on which the images were shared,
- f. and data security/management protocols around the handling of the shared data.

Clarification from you the requester :

Unfortunately that FOI response does not address my FOI request, which deals with police provision of photos given to external facial recognition operators. I would be grateful if you could progress my FOI request.

Answers 2 – 9

No.

In addition to the responses provided above, PSNI neither confirms nor denies that it holds any other information relevant to the request.

Section 1 of the Freedom of Information Act 2000 (FOIA) 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 the 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(1) of FOIA requires that we provide the applicant with

a notice which

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

Section 24(1) National Security - Information which does not fall within Section 23(1) is exempt information if exemption from section 1(1)(b) is required for the purpose of safeguarding national security.

Section 31(3) Law Enforcement - 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).

The full text of exemptions can be found at www.legislation.gov.uk and further guidance on how they operate can be located on the Information Commissioners Office website www.ico.org.uk.

Sections 24 and 31 are prejudice based qualified exemptions and there is a requirement to articulate the harm that would be caused in confirming or denying that any other information is held as well as carrying out a public interest test.

Harm for partial NCND

Any disclosure under FOI is a release to the public at large. Whilst not questioning the motives of the applicant, confirming or denying that any other information relating to the covert practise of Facial Recognition (FR) 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 FR 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 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 this 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'.

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 FR 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 information can be of use 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.

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.

Factors Favouring Neither Confirming Nor Denying for Section 24

The information if held simply relates to national security and confirming or denying whether it is held would not actually harm it. The public are entitled to know what public funds are spent on and what security measures are in place, and by confirming or denying whether any other information regarding the covert use of FR is held, would lead to a better informed public.

Factors Against Neither Confirming Nor Denying for Section 24

By confirming or denying whether any other information is held would render security measures less effective. This would lead to the compromise of ongoing or future operations to protect the security or infrastructure of the UK and increase the risk of harm to the public.

Factors Favouring Neither Confirming Nor Denying for Section 31

Confirming or denying whether any other information is held regarding the covert use of FR would provide an insight into the police service. This would enable the public to have a better understanding of the effectiveness of the police. It would greatly assist in the quality and accuracy of public debate, which could otherwise be steeped in rumour and speculation. Where public funds are being spent, there is a public interest in accountability and justifying the use of public money.

Some information is already in the public domain regarding the police use of this type of specialist equipment and confirming or denying whether any other information is held would ensure transparency and accountability and enable the public to see what tactics are deployed by the Police Service to detect crime.

Factors Against Neither Confirming Nor Denying for Section 31

Confirming or denying that any other information is held regarding the covert use of FR would have the effect of compromising law enforcement tactics and would also hinder any future investigations. In addition, confirming or denying methods used to gather intelligence for an investigation would prejudice that investigation and any possible future proceedings.

It has been recorded that FOIA releases are monitored by criminals and terrorists and so to confirm or deny any other information is held concerning specialist covert tactics would lead to law enforcement being undermined. The Police Service is reliant upon all manner of techniques during operations and the public release of any other information, if held, would prejudice the ability of the Police Service to conduct investigations.

By confirming or denying whether any other information is held in relation to the covert use of FR would hinder the prevention or detection of crime. The Police Service would not wish to reveal what tactics may or may not have been used to gain intelligence as this would clearly undermine the law enforcement and investigative process. This would impact on police resources and more crime and terrorist incidents would be committed, placing individuals at risk. It can be argued that there are significant risks associated with providing information, if held, in relation to any aspect of investigations or of any nation's security arrangements so confirming or denying that any other information is held, may reveal the relative vulnerability of what we may be trying to protect.

Decision

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 regarding the covert use of FR if to do so would place the safety of an individual at risk, undermine National Security or compromise law enforcement.

Whilst there is a public interest in the transparency of policing operations and providing assurance that the police service is appropriately and effectively engaging with the threat posed by various groups or individuals, there is a very strong public interest in safeguarding the integrity of police

investigations and operations in the highly sensitive areas such as extremism, crime prevention, public disorder and terrorism prevention.

As much as there is public interest in knowing that policing activity is appropriate and balanced this will only be overridden in exceptional circumstances. The areas of police interest discussed above are sensitive issues that reveal local intelligence and therefore it is our opinion that for these issues the balancing test for confirming or denying whether any other information is held regarding the covert use of FR, is not made out.

However, this should not be taken as necessarily indicating that any information that would meet your request exists or does not exist.

If you have any queries regarding your request or the decision please do not hesitate to contact me on 028 9070 0164. When contacting the Freedom of Information Team, please quote the reference number listed at the beginning of this letter.

If you are dissatisfied in any way with the handling of your request, you have the right to request a review. You should do this as soon as possible or in any case within two months of the date of issue of this letter. In the event that you require a review to be undertaken, you can do so by writing to the Head of Freedom of Information, PSNI Headquarters, 65 Knock Road, Belfast, BT5 6LE or by emailing foi@psni.pnn.police.uk.

If following an internal review, carried out by an independent decision maker, you were to remain dissatisfied in any way with the handling of the request you may make a complaint, under Section 50 of the Freedom of Information Act, to the Information Commissioner's Office and ask that they investigate whether the PSNI has complied with the terms of the Freedom of Information Act. You can write to the Information Commissioner at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. In most circumstances the Information Commissioner will not investigate a complaint unless an internal review procedure has been carried out, however the Commissioner has the option to investigate the matter at his discretion.

Please be advised that PSNI replies under Freedom of Information may be released into the public domain via our website @ www.psni.police.uk

Personal details in respect of your request have, where applicable, been removed to protect confidentiality.