18th December 2020

Freedom of Information Request - Reference No: 20202446

REQUEST

1) Does the police force know what percentage of computers in use by the force continue to use legacy operating systems? (Legacy defined as Windows XP or older) If so, please disclose that percentage.

2) Please disclose whether your police force has developed/implemented, is in the process of developing/implementing, or is not developing/implementing the following technologies (listed below, brief summaries included for your convenience).

- ***Augmented Reality and/or Virtual Reality***
- ***Artificial Intelligence***
- ***Biometrics (technology used to identify individual by their unique physical and behavioural traits)***
- ***Case Assessment Tools (An algorithm to assess cases based on their apparent solvability)***
- ***Citizen Relationship Management (processes that allow police to build a picture of the individuals they are interacting with by showing a history of past interactions with the police)***
- ***Cloud technology***
- ***Crime prediction technology***
- ***Cyber Security (National Management Centre)***
- ***Data analytic capabilities (processes which enable the automation of routine processing and the generation of insight on a vast range of policing problems***
- ***Digital forensics***
- ***Drones (unmanned aerial vehicles)***
- ***Facial recognition technology***
- ***Mobile working tools***
- ***Robotic process automation (the use of 'digital workers' to automate repetitive tasks to free up staff for other duties)***
- ***Video hearings***
- ***Wearable working tools (including bodycams)***

CLARIFICATION

South Yorkshire Police has received a number of similar requests to yours in the past. …..this type of data may be sensitive data we wouldn't release into the public domain, the following links cover some of the detail you require: -

https://www.southyorkshire.police.uk/find-out/accessing-information/request-information-under-the-freedom-of-information-act/artificial-intelligence-ref-20192577/

https://www.southyorkshire.police.uk/find-out/accessing-information/request-information-under-the-freedom-of-information-act/police-computer-systems-ref-20191251/

FROM THE REQUESTER

Please see amended request below:

1) Does the police force know what percentage of computers in use by the force continue to use legacy operating systems? (Legacy defined as Windows XP or older) If so, please disclose that percentage.

2) Please disclose whether your police force has developed/implemented, is in the process of developing/implementing, or is not developing/implementing the following technologies (listed below, brief summaries included for your convenience).

- ***Augmented Reality and/or Virtual Reality***
- ***Biometrics (technology used to identify individual by their unique physical and behavioural traits)***
- ***Case Assessment Tools (An algorithm to assess cases based on their apparent solvability)***
- ***Citizen Relationship Management (processes that allow police to build a picture of the individuals they are interacting with by showing a history of past interactions with the police)***
- ***Cloud technology***
- ***Cyber Security (National Management Centre)***
- ***Data analytic capabilities (processes which enable the automation of routine processing and the generation of insight on a vast range of policing problems***
- ***Digital forensics***
- ***Drones (unmanned aerial vehicles)***
- ***Mobile working tools (for use by officers on the beat, rather than within the office environment)***
- ***Robotic process automation (the use of 'digital workers' to automate repetitive tasks to free up staff for other duties)***
- ***Video hearings***
- ***Wearable working tools (including bodycams)***

RESPONSE

In respect of Q1:

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 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 FOIA 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 exemptions apply.

South Yorkshire Police neither confirms nor denies that it holds further information relevant to this request by virtue of:

Section 24(2) National Security
Section 31(3) Law Enforcement
Sections 24 and 31 being prejudice based qualified exemptions, both evidence of harm and public interest considerations need to be articulated to the applicant.

Harm in Confirming or Denying that Information is held

Policing is an information-led activity, and information assurance (which includes information security) is fundamental to how the Police Service manages the challenges faced. In order to comply with statutory requirements, the College of Policing Authorised Professional Practice for Information Assurance has been put in place to ensure the delivery of core operational policing by providing appropriate and consistent protection for the information assets of member organisations, see below link:

https://www.app.college.police.uk/app-content/information-management/

To confirm or deny whether South Yorkshire Police uses a certain operating system would identify vulnerable computer systems and provide actual knowledge, or not, that this software is used within individual force areas. In addition, this would have a huge impact on the effective delivery of operational law enforcement as it would leave forces open to cyberattack which could render computer devices obsolete.

This type of information would be extremely beneficial to offenders, including terrorists and terrorist organisations. It is vitally important that information sharing takes place with other police forces and security bodies within the UK to support counter-terrorism measures in the fight to deprive terrorist networks of their ability to commit crime.

To confirm or deny whether or not South Yorkshire Police relies on a certain operating system would be extremely useful to those involved in terrorist activity as it would enable them to map vulnerable information security databases.

Public Interest Considerations

Section 24(2) National Security

Factors favour complying with Section 1(1)(a) confirming that information is held

The public are entitled to know how public funds are spent and how resources are distributed within an area of policing. To confirm whether South Yorkshire Police utilises Windows XP/7 would enable the general public to hold South Yorkshire Police to by highlighting forces who use out of date software. In the current financial climate of cuts and with the call for transparency of public spending this would enable improved public debate into this subject.

Factors against complying with Section 1(1)(a) confirming or denying that information is held

Security measures are put in place to protect the community we serve. As evidenced within the harm to confirm information is held would highlight to terrorists and individuals intent on carrying out criminal activity vulnerabilities within South Yorkshire Police.
Taking into account the current security climate within the United Kingdom, no information (such as the citing of an exemption which confirms information pertinent to this request is held, or conversely, stating “no information is held”)which may aid a terrorist should be disclosed. To what extent this information may aid a terrorist is unknown, but it is clear that it will have an impact on a force’s ability to monitor terrorist activity.

Irrespective of what information is or isn’t held, the public entrust the Police Service to make appropriate decisions with regard to their safety and protection and the only way of reducing risk is to be cautious with what is placed into the public domain.

The cumulative effect of terrorists gathering information from various sources would be even more impactive when linked to other information gathered from various sources about

terrorism. The more information disclosed over time will give a more detailed account of the tactical infrastructure of not only a force area, but also the country as a whole.

Any incident that results from such a disclosure would, by default, affect National Security.

Section 31(3) Law Enforcement

Factors favouring complying with Section 1(1)(a) confirming that information is held

Confirming that information exists relevant to this request would lead to a better informed public which may encourage individuals to provide intelligence in order to reduce the risk of police networks being hacked.

Factors against complying with Section 1(1)(a) neither confirming nor denying that information is held

Confirmation or denial that information is held in this case would suggest South Yorkshire Police take their responsibility to protect information and information systems from unauthorised access, destruction, etc., dismissively and inappropriately.

Balancing Test

The points above highlight the merits of confirming or denying the requested information exists. The Police Service is charged with enforcing the law, preventing and detecting crime and protecting the communities we serve. As part of that policing purpose, information is gathered which can be highly sensitive relating to high profile investigative activity.

Weakening the mechanisms used to monitor any type of criminal activity, and specifically terrorist activity would place the security of the country at an increased level of danger.

In order to comply with statutory requirements and to meet NPCC expectation of the Police Service with regard to the management of information security a national policy approved by the College of Policing titled National Policing Community Security Policy has been put in place. This policy has been constructed to ensure the delivery of core operational policing by providing appropriate and consistent protection for the information assets of member organisations. A copy of this can be found at the below link:

http://library.college.police.uk/docs/APP-Community-Security-Policy-2014.pdf

In addition, anything that places that confidence at risk, no matter how generic, would undermine any trust or confidence individuals have in the Police Service. Therefore, at this moment in time, it is our opinion that for these issues the balance test favours neither confirming nor denying that information is held.

In respect to the other information requested:

I approached our IT Department and Specialist Crime Services for assistance with your request. Please see the following details provided to me:

2) Please disclose whether your police force has developed/implemented, is in the process of developing/implementing, or is not developing/implementing the following technologies (listed below, brief summaries included for your convenience).

- ***Augmented Reality and/or Virtual Reality NO – SCS are not involved in any of this activity nor are we planning to be involved in any of this activity***
- ***Biometrics (technology used to identify individual by their unique physical and behavioural traits) Yes, in process of developing (irt mobile fingerprint scanners***
- ***Case Assessment Tools (An algorithm to assess cases based on their apparent solvability) No***
- ***Citizen Relationship Management (processes that allow police to build a picture of the individuals they are interacting with by showing a history of past interactions with the police) -No***
- ***Cloud technology Yes***
- ***Cyber Security (National Management Centre) Yes***
- ***Data analytic capabilities (processes which enable the automation of routine processing and the generation of insight on a vast range of policing problems Yes – we do use analytic capabilities as part of business as usual***
- ***Digital forensics Yes***
- ***Drones (unmanned aerial vehicles) Yes***
- ***Mobile working tools (for use by officers on the beat, rather than within the office environment)Yes mobile phone and laptops***
- ***Robotic process automation (the use of 'digital workers' to automate repetitive tasks to free up staff for other duties) In the process of***
- ***Video hearings Yes***
- ***Wearable working tools (including bodycams) Yes***

Augments or Virtual Reality / Data Analytics – https://www.southyorkshire.police.uk/find-out/accessing-information/request-information-under-the-freedom-of-information-act/artificial-intelligence-ref-20192577/

https://www.southyorkshire.police.uk/media/4496/1829_force_management_statement_2019_03.pdf

Algorithms – https://www.southyorkshire.police.uk/find-out/accessing-information/request-information-under-the-freedom-of-information-act/algorithms-technology-ref-20181279/

In addition, in regard to any further information, South Yorkshire Police force neither confirms nor denies that it holds any other information relevant to the request by virtue of the following exemptions:

Section 23(5) - Information supplied by, or concerning, certain security bodies
Section 24(2) - National Security
Section 31(3) - Law Enforcement

Section 23 is a class based absolute exemption and there is no requirement to consider the public interest in this case. Confirming or denying the existence of whether any other information is held would contravene the constrictions laid out within Section 23 of the Freedom of Information Act 2000 in that this stipulates a generic bar on disclosure of any information applied by, or concerning, certain Security Bodies.

Overall Harm

Sections 31 and 24 are prejudice based qualified exemptions and there is a requirement to evidence the prejudice (harm) in disclosure and consider the public interest to ensure neither confirming or denying that any other information is held is appropriate.

As you will be aware, disclosure under FOIA is a release to the public at large. Whilst not questioning the motives of the applicant, confirming or denying that any other information is held regarding the use of this specialist equipment for covert practise, 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 drones, 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 have 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 2017 following the Manchester Bombing, when it was raised to the highest threat, 'critical', it has since been reduced to 'substantial'. Nevertheless, the UK continues to face a sustained threat from violent extremists and terrorists and the current UK 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 that any other information is held in relation to the covert use of drones, unmanned aerial devices, would limit operational capabilities as criminals/terrorists would gain a greater understanding of the police forces' methods and techniques, enabling them 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.
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.

Public Interest Test
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 is held regarding the covert use of drones, 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 infra-structure 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 drones would provide an insight into the Police Service. This would enable the public to have a better understanding of the effectiveness of the police and about how the police gather intelligence. 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 these type of specialist equipment/technology 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 drones 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 modus operandi employed, if held, would prejudice the ability of the Police Service to conduct similar investigations.

By confirming or denying whether any other information is held in relation to the covert use of drones 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.

Balance test

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 drones 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 all areas of operations carried out by police forces throughout the UK.

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 use of drones in any covert capacity is a sensitive issue that would reveal police tactics 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 drones, 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.