Request Reference: 10016/19

Request

2) Which is the prevalent computer operating system across the constabulary (for example Microsoft Windows XP, WIndows7, Windows 10, iOS (Apple), Chrome or other);

3) Which version of that system is the default;

4) Regardless which system is the current default, whether there is an intention to move to Windows 10 and if so when and at what estimated cost.

5) If the force has commenced this move to Windows 10, what approximate proportion of devices are using Windows 10.

Applicable exemptions:

Section 24(2) - National security

Section 31(3) - Law enforcement

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 West Midlands 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 West Midlands 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 favouring complying with Section 1(1)(a) confirming or denying 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 West Midlands Police utilises specific software would enable the general public to hold West Midlands 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) - neither 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 West Midlands 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 or denying 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 West Midlands Police take their responsibility to protect information and information systems from unauthorised access, destruction, etc., dismissively and inappropriately.

Balance Test

For this public interest test, factors favouring complying with Section 1(1)(a) - confirming or denying that information is held, need to be measured against factors against complying with Section 1(1)(a) - neither confirming nor denying that information is held. The public interest is not what interests the public, or a particular individual, but what will be the greater good, if released, to the community as a whole.

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 it is my opinion that for these factors the public interest in maintaining the exemption outweighs the public interest in disclosure.