



FREEDOM OF INFORMATION REQUEST



Request Number: F-2018-00493

Keyword: Crime

Subject: Computer Misuse Act

Request and Answer:

Request 1

The number of crimes reported to your police force which fall under the Computer Misuse Act in each of the last 3 years (2015, 2016, 2017)?

Request 2

Of those crimes reported the number which references the following terms in initial police reports: "Hacking", "Smart device", "Connected device".

Request 3

Summary details on the crimes reported in 1 and 2.

Request 4

Outcomes of those crimes reported in 1 and 2.

Request 5

The number of crimes reported to your police force which fall under the Computer Misuse Act and makes reference to the following in each of the last 3 years (2015, 2016, 2017): "Jump box", "Penetration test drop box", "Drop box", "Raspberry pi".

Request 6

Summary details on the crimes reported in 5.

Request 7

Outcomes of those crimes reported in 5.

Request 8

The number of crimes reported to your police force which fall under the Computer Misuse Act which are classified as "denial of service" attack in each of the last 3 years (2015, 2016, 2017).

Request 9

Summary details on the crimes reported in 8.

Request 10

Outcomes of those crimes reported in 8.

Answer

Searches were conducted however these searches failed to locate any records or documents relevant to your request based on the information you have provided. Information is not recorded on Niche, our Record Management System in a way that makes it possible to search for offences under the Computer Misuse Act. Action Fraud records these offences on behalf of the Police Service of Northern Ireland (PSNI). Accordingly, I have determined that the PSNI does not hold the information to which you seek access.

In addition, PSNI neither confirms nor denies that it holds any other information relevant to offences under the Computer Misuse Act by virtue of the following exemptions:

Section 24(2) National Security - The duty to confirm or deny does not arise if, or to the extent that, exemption from Section 1(1)(a) 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

'Neither Confirm nor Deny' (NCND)

There may be occasions when complying with the duty to confirm or deny under Section 1(1)(a) of the Freedom of Information Act 2000 (FOIA) would in itself disclose sensitive or potentially damaging information that falls under an exemption. In these circumstances the FOIA allows a public authority to respond by refusing to confirm or deny whether it holds the requested information.

The decision to issue a 'neither confirm nor deny' response is not affected by whether we do or do not hold the information but relates to the consequences of confirming or denying the information is held. The starting point and main focus in most cases will be theoretical considerations about the consequences of confirming or denying that a particular type of information is held. The decision to neither confirm nor deny is separate from a decision not to disclose information and needs to be taken entirely on its own merits.

PSNI follow the Information Commissioner's Guidance in relation to 'NCND' and you may find it helpful to refer to this at the following link:

[https://ico.org.uk/media/for-organisations/documents/1166/when to refuse to confirm or deny section 1 foia.pdf](https://ico.org.uk/media/for-organisations/documents/1166/when_to_refuse_to_confirm_or_deny_section_1_foia.pdf)

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

Harm

The release of information under the FOIA is a release into the public domain and not just to the individual making the request. Any information relating to computer misuse is likely to be sensitive and once information is disclosed under the FOIA there is no control or limits as to who or how the information is shared with other individuals, therefore such a release is considered a disclosure to the world in general. To confirm or deny whether or not PSNI hold any other information relating to computer misuse has the potential to disclose sensitive or potentially damaging information which would undermine policing across the UK and impact national security.

Public Interest Test

Factors Favouring Confirmation or Denial Section 24

The public are entitled to know how public funds are spent and confirmation or denial that any other information is held relating to computer misuse would better inform the public of how this money is being spent. Confirmation that PSNI is actively working to safeguard the public against the threat of terrorism may also enhance public confidence in PSNI.

Factors Against Confirmation or Denial Section 24

To confirm or deny that any other information is held would render security measures less effective which would compromise ongoing or future operations to protect the security and infrastructure of the UK.

Factors Favouring Confirmation or Denial Section 31

Confirming or denying whether or not any other information is held relating to computer misuse would enhance the PSNI's transparency and accountability. Improved public awareness may lead to more intelligence being submitted to police which in turn may result in a reduction of crime.

Factors Against Confirmation or Denial Section 31

To confirm or deny that any other information is held would compromise law enforcement tactics which would hinder PSNI's ability to prevent and detect crime. This would be detrimental to providing an efficient policing service.

Decision

The security of the country is of paramount importance and PSNI will not divulge whether any other information is or is not held relating to computer misuse if to do so would undermine national security, place the safety of individuals at risk or compromise law enforcement. Whilst there is a public interest in transparency and in demonstrating that PSNI is justified and accountable in the use of public funds there is a very strong public interest in safeguarding both national security and law enforcement tactics.

The international security landscape is increasingly complex and unpredictable and the threat from terrorism cannot be ignored. The UK faces a sustained threat from violent terrorists and extremists. Since 2006, the UK Government has published the threat level as set by the security service (MI5) based upon current intelligence. The threat level to the UK is currently 'severe', the Home Office website explains 'this means that a terrorist attack is highly likely'.

<http://www.homeoffice.gov.uk/counter-terrorism/current-threat-level/>

The PSNI is charged with enforcing the law, preventing and detecting crime and protecting the public and to confirm or deny that any other information is held on this topic would hinder PSNI's law enforcement abilities which would be detrimental to providing an efficient policing service.

Taking all these factors into consideration, I am satisfied that the exemptions outlined above are applicable to this request therefore the public interest must favour neither confirming nor denying that any other information is held. This should not be taken as conclusive evidence that any other information does 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.