| Police Scotland logo | Freedom of Information Response Our reference: FOI 23-0364  Responded to: 20th March 2023 |
| --- | --- |

Your recent request for information is replicated below, together with our response.

**I am looking for information on digital forensics. The information/ question I am looking for information are as follows:**

**1. How many digital forensic officers are able to gather data from smart home devices within the digital forensic unit?**

Following a clarification request you confirmed that by smart home devices, you were referring to smart speakers, doorbells, fridges, and watches. This definition has been used throughout your whole request.

I can confirm that all of our digital forensic staff can gather data from the devices requested.

In relation to the specific number of staff this refers to, the requested information is considered to be exempt in terms of the Freedom of Information (Scotland) Act 2002 (the Act). Section 16 of the Act requires Police Scotland to provide you with a notice which:

* states that it holds the information,
* states that it is claiming an exemption,
* specifies the exemption in question and
* states, if that would not be otherwise apparent, why the exemption applies.

Where information is considered to be exempt, this letter serves as a Refusal Notice that information is held and an explanation of the appropriate exemption is provided.

The exemptions that I consider to be applicable to the information requested by you are:

## Section 35 (1) (a) & (b) – Law Enforcement

The information requested is exempt, as its disclosure would or would be likely to prejudice substantially the prevention or detection of crime and apprehension or prosecution of offenders. If the details of Police Scotland’s cybercrime resourcing was disclosed, experience has shown that it would allow those intent on committing crime or causing disorder to gauge the likelihood of detection or to take measures to negate the likelihood of detection. It would allow criminals to plan how best to engage or occupy existing police resources in an effort to maximise their chances of committing serious crime, therefore harming the efficient and effective conduct of the service.

Such information would prove extremely useful information for persons involved in criminality as they would be able to plan and conduct their activities to avoid detection. It would confirm the resources available in a specialised area of policing, which would allow those intent on wrong doing to judge the police response to a variety of incidents. In turn this would prejudice substantially the ability for our officers to prevent and detect crime and apprehend or prosecute offenders.

Disclosure would have an adverse impact on the ability of the Police to carry out its law enforcement role effectively, and thereby prejudice substantially the prevention and detection of crime.

This is a non-absolute exemption and requires the application of the public interest test.

## Section 39(1) – Health, safety and the environment

Disclosure of the information requested would prove extremely useful for criminals and those intent on wrongdoing, to estimate the level of cybercrime resources deployed by the Police and would assist them in circumventing the efficient and effective provision of law enforcement by the police service, which in turn would have an adverse impact on the safety of the officers involved and the general public.

This would increase the risk to the personal safety of individuals and also the safety of the police officers responding to incidents.

This is a non-absolute exemption and requires the application of the public interest test.

## Public Interest Test

As you will be aware, the two exemptions detailed above are non-absolute and require the application of the public interest test. Public awareness would favour a disclosure as it would contribute to the public debate surrounding the use and deployment of unit and vehicle resources by the Police, particularly specialist vehicles.

I would, however, contend that the efficient/effective conduct of the service and public safety favours retention of the information as it cannot be in the public interest to release information that would prejudice law enforcement or which is likely to have an adverse impact upon public safety.

**2. What are the issues the digital forensic unit faces when analysing data from smart home devices?**

I must conclude that as it does not seek a copy of recorded information, it is not a valid request in terms of Section 8 of the Freedom of Information (Scotland) Act 2002.

By way of explanation, your question is seeking an opinion which is not considered recorded information as per the Act.

**3. What are the procedures, principles and legislation that must be adhered to when handling, obtaining and analysing digital smart home devices within the digital forensic unit?**

In regards to the principles and legislation we adhere to when analysing digital smart home devices, I can confirm we use the [ACPO Good Practice Guide for Digital Evidence](https://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf)

In regards to the specific procedures we adhere to, the requested information is considered to be exempt in terms of the Freedom of Information (Scotland) Act 2002 (the Act). Section 16 of the Act requires Police Scotland to provide you with a notice which:

* states that it holds the information,
* states that it is claiming an exemption,
* specifies the exemption in question and
* states, if that would not be otherwise apparent, why the exemption applies.

Where information is considered to be exempt, this letter serves as a Refusal Notice that information is held and an explanation of the appropriate exemption is provided.

The exemptions that I consider to be applicable to the information requested by you are:

**Section 31(1) – National Security and Defence**

Information is exempt information if exemption from section 1(1) is required for the purpose of safeguarding national security.

If the information is disclosed it may assist terrorist organisations to identify, with some accuracy the capabilities of our cybercrime department and as such would allow them to carry out their criminal or terrorist activities.

This is a non-absolute exemption and requires the application of the public interest test.

**Section 35 (1) (a) & (b) – Law Enforcement**

The information requested is exempt, as its disclosure would or would be likely to prejudice substantially the prevention or detection of crime and apprehension or prosecution of offenders. If the details of Police Scotland’s cybercrime capabilities was disclosed, experience has shown that it would allow those intent on committing crime or causing disorder to gauge the likelihood of detection or to take measures to negate the likelihood of detection. It would allow criminals to plan how best to avoid detection in an effort to maximise their chances of committing serious crime, therefore harming the efficient and effective conduct of the service.

Disclosure would have an adverse impact on the ability of the Police to carry out its law enforcement role effectively, and thereby prejudice substantially the prevention and detection of crime.

This is a non-absolute exemption and requires the application of the public interest test.

**Section 39(1) – Health, safety and the environment**

Disclosure of the information requested would prove extremely useful for criminals and those intent on wrongdoing, to estimate the capabilities of cybercrime resources deployed by the Police and would assist them in circumventing the efficient and effective provision of law enforcement by the police service, which in turn would have an adverse impact on the safety of the officers involved and the general public.

This would increase the risk to the personal safety of individuals and also the safety of the police officers responding to incidents.

This is a non-absolute exemption and requires the application of the public interest test.

**Public Interest Test**

As you will be aware, the two exemptions detailed above are non-absolute and require the application of the public interest test. Public awareness would favour a disclosure as it would contribute to the public debate surrounding the use and deployment of our cybercrime unit and provide additional information on their capabilities and remit.

I would, however, contend that the efficient/effective conduct of the service and public safety favours retention of the information as it cannot be in the public interest to release information that would prejudice law enforcement or which is likely to have an adverse impact upon public safety.

**4. What software/ hardware is used to analyse and extract data from smart home devices?**

The requested information is considered to be exempt in terms of the Freedom of Information (Scotland) Act 2002 (the Act) under sections 31(1), 35(1)(a)&(b) and 39(1). I would direct you to my rationale within the exemptions applied to question 3 for the reasons for this.

**5. Is the digital forensic laboratory software/ hardware used accredited under the accreditation ISO17025?**

Yes.

**6. Are write blockers used to analyse data obtained from smart home devices?**

Having considered your request in terms of the Freedom of Information (Scotland) Act 2002, I am refusing to confirm or deny whether the information sought exists or is held by Police Scotland in terms of section 18 of the Act.

Section 18 applies where the following two conditions are met:

- It would be contrary to the public interest to reveal whether the information is held

Whilst we accept that you may have a particular personal interest in being informed as to whether or not the information sought is held, the overwhelming public interest lies in protecting individuals’ right to privacy and the expectation of confidence that the public have in Police Scotland as regards their information.

- If the information was held, it would be exempt from disclosure in terms of one or more of the exemptions set out in sections 28 to 35, 38, 39(1) or 41 of the Act If you require any further assistance please contact us quoting the reference above.

In this case sections 31(1), 35(1)(a)&(b) and 39(1) would apply. I would direct you to my rationale within the exemptions applied to question 3 for the reasons for this.

I would emphasise that our response does not confirm whether Police Scotland holds the requested information or not.

You can request a review of this response within the next 40 working days by [email](mailto:foi@scotland.police.uk) or by letter (Information Management - FOI, Police Scotland, Clyde Gateway, 2 French Street, Dalmarnock, G40 4EH). Requests must include the reason for your dissatisfaction.

If you remain dissatisfied following our review response, you can appeal to the Office of the Scottish Information Commissioner (OSIC) within 6 months - [online](http://www.itspublicknowledge.info/Appeal), by [email](mailto:enquiries@itspublicknowledge.info) or by letter (OSIC, Kinburn Castle, Doubledykes Road, St Andrews, KY16 9DS).

Following an OSIC appeal, you can appeal to the Court of Session on a point of law only.

This response will be added to our [Disclosure Log](http://www.scotland.police.uk/access-to-information/freedom-of-information/disclosure-log) in seven days' time.

Every effort has been taken to ensure our response is as accessible as possible. If you require this response to be provided in an alternative format, please let us know.