| Police Scotland logo | Freedom of Information ResponseOur reference: FOI 24-2748Responded to: 06 November 2024 |
| --- | --- |

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

**I would like to request the following information for the period from January 1, 2019, to December 31, 2023:**

**1. Number of Mobile Devices Analysed: The total number of mobile devices (e.g., smartphones, tablets) submitted to Police Scotland for digital forensic analysis each year between 2019 and 2023. Please provide this data broken down by year.**

For the purposes of this request, we have interpreted the term ‘mobile device’ as meaning the following devices:

* Mobile Telephones
* SIM Cards
* Satellite Navigation Devices (Sat Navs)
* Tablets.

Table 1 below details the number of Examination Request Forms (ERFs) approvedandthe number ofmobile devices analysed by Police Scotland, by calendar year for the period 01/01/2019 to 31/12/2023.

Please note that an Examination Request Form may refer to more than one device.

Table 1

|  |  |  |
| --- | --- | --- |
| **Year** | **Cybercrime ERFs Approved** |  **‘Mobile Devices’ Approved for Examination** |
| 2019 | 5653 | 11225 |
| 2020 | 5847 | 11931 |
| 2021 | 6269 | 11736 |
| 2022 | 6036 | 10990 |
| 2023 | 5936 | 10993 |

**2. Types of Devices: If available, a breakdown of the types of mobile devices analysed (e.g., iOS devices, Android devices, other operating systems) for each year from 2019 to 2023.**

Police Scotland to not routinely record information regarding the operating systems used by the devices and section 17 of the act therefore applies.

To be of assistance, table 2 below provides a breakdown of analysed devices by device type per year.

Table 2

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Year** |  **Mobile Telephones** | **SIM Cards** | **Sat Navs** | **Tablets** | **Total** |
| 2019 | 9974 | 341 | 34 | 876 | 11225 |
| 2020 | 10705 | 404 | 33 | 789 | 11931 |
| 2021 | 10669 | 357 | 15 | 695 | 11736 |
| 2022 | 10048 | 310 | 3 | 629 | 10990 |
| 2023 | 10059 | 386 | 17 | 531 | 10993 |

**3. Success Rates of Data Extraction: The percentage of cases where usable data was successfully extracted from the mobile devices submitted for forensic analysis, broken down by year. If success rates are tracked differently (e.g., by extraction method), please provide a description of the methodology used.**

Unfortunately, I estimate that it would cost well in excess of the current FOI cost threshold of £600 to process your request.

I am therefore refusing to provide the information sought in terms of section 12(1) - Excessive Cost of Compliance.

To explain, the only way to answer this part of your request would be to research each of the thousands of cases referred to above individually and extract and note the relevant data.

**4. Encryption Challenges: If available, the number or percentage of cases where digital forensics was unable to retrieve data from a mobile device due to encryption or other technical barriers, broken down by year.**

Police Scotland’s Cybercrime Investigations and Digital Forensics Unit consistently review and update technologies, policies and procedures to ensure that they remain able and equipped to investigate serious crime.

Unfortunately, however, I estimate that it would cost well in excess of the current FOI cost threshold of £600 to process your request.

I am therefore refusing to provide the information sought in terms of section 12(1) - Excessive Cost of Compliance.

To explain, the only way to answer this part of your request would be to research each of the thousands of cases referred to above individually and extract and note the relevant data.

**5. Data Types Extracted: Information on the types of data most commonly extracted from mobile devices during forensic analysis (e.g., call logs, text messages, app data, location data, images), and any notable changes in data extraction trends over the specified period.**

Police Scotland’s Cybercrime Investigations and Digital Forensics Unit analyse devices to extract relevant data in relation to the investigation at hand, as directed by the Investigating Officer, Senior Investigating Officer and/or Crown Office and Procurator Fiscals Service (COPFS).

Unfortunately, however, I estimate that it would cost well in excess of the current FOI cost threshold of £600 to process your request.

I am therefore refusing to provide the information sought in terms of section 12(1) - Excessive Cost of Compliance.

To explain, the only way to answer this part of your request would be to research each of the thousands of cases referred to above individually and extract and note the relevant data.

**6. Use of External Tools or Vendors: Please indicate whether Police Scotland has outsourced any mobile device analysis to third-party digital forensic firms or used any external tools during the data extraction process, and if so, provide details on the number of cases where this was necessary.**

Police Scotland do not outsource digital forensic examinations. All devices are examined internally.

**7. Technological Challenges: Any internal reports, summaries, or assessments that highlight technological challenges or barriers Police Scotland has faced when extracting data from mobile devices over the specified period, including cases where analysis was not possible due to device lockout, encryption, or other factors**

The information sought is held by Police Scotland, but I am refusing to provide it in terms of section 16(1) of the Act on the basis that the following exemptions apply:

* Section 31(1) - National Security and Defence
* Section 35(1)(a)&(b) - Law enforcement

Exemption is required for the purpose of safeguarding national security and, additionally, disclosure would prejudice substantially the prevention or detection of crime and the apprehension or prosecution of offenders.

Disclosure would assist groups, organisations and those with hostile intent to identify, with some accuracy Police Scotland’s Cyber analysis capabilities. This would undermine any ongoing or future operations to protect the security or infrastructure of the United Kingdom and increase the risk of harm to the public.

Disclosure would facilitate criminal activities, thereby compromising the effective delivery of operational law enforcement.

*Public Interest Test*

Public awareness would favour a disclosure as it would contribute to the public debate surrounding Cyber security.

That said, I would contend that the efficient/effective conduct of the service and national security favours non-disclosure 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 national security.

If you require any further assistance, please contact us quoting the reference above.

You can request a review of this response within the next 40 working days by email 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 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.