



Police Headquarters
London Road
DEVIZES
Wiltshire
SN10 2DN

Date: December 16, 2025

Our ref: FOI 2025/877

Reply contact name:

Dear,

I write in connection with your request for information dated 9th September 2025 concerning mobile phone data extraction.

I am required by the Freedom of Information Act 2000 to handle all requests in a manner that is blind as to the identity and motives of the requestor. Any information released as a response to a request is regarded as being published and therefore in the public domain without caveat.

Your request for information has now been considered and I am able to respond as follows.

You Wrote:

I am writing to ask that you provide me with the following information on your use of mobile phone data extraction:

1. Does your police force currently carry out mobile phone data extraction in low level crime cases using self-service / downloading kiosks? Please provide your definition of low-level crime.
2. Does your police force currently carry out mobile phone data extraction in serious crimes using self-service / downloading kiosks?
3. If your police force is not currently using mobile phone extraction kiosks, have you trialled this in the past/do you have plans to in the future?
4. Does your police force currently use Hubs to carry out mobile phone data extraction in (a) low-level crimes? (b) serious crimes?
5. Do you centrally record mobile phone data extracted from kiosks?
6. If you have a mobile phone extraction kiosk, please provide the name of the company(ies) which currently provide(s) the hardware / software / to whom you pay a

license for the relevant tools. If contracts for these tools exist, please also provide the beginning and end dates of these.

7. Does your police force use analytics software to process, analyse or evaluate data extracted from mobile phones? If so, please provide the name of the software or provider.

8. How many officers currently carry mobile phone examination kits on patrol and/or in vehicles and/or for other operational use in (a) low level crimes? (b) serious crimes?

9. Please confirm whether or not a review has been conducted into the use of self-service kiosks.

10. Please provide copies of the current relevant force level and/or national level guidance for the use of downloading kiosks.

11. Please provide copies of the current relevant force level and/or national level policy for the use of downloading kiosks.

Your response cited Section 24 (National Security) and Section 31 (Law Enforcement). As both exemptions are qualified exemptions, you are required to demonstrate that the disclosure would be likely to cause specific, identifiable prejudice, and that the public interest in maintaining the exemption outweighs the public interest in disclosure. I do not believe the response meets these statutory requirements.

The public interest test has not been adequately evidenced - as the test presented does not appear to be balanced. There seems to have been an inflated idea of how knowledge of the companies used would aid in criminal activity, or activity that could threaten national security.

There also has not been a consideration of a partial disclosure, e.g. disclosing the company but not the specific system or technology used.

Response:

On reviewing your original Freedom of Information request, the response provided and your request for an Internal Review, I can respond as follows:

I believe that the exemptions used for Question Seven have been incorrectly applied in full, and that we should have confirmed that the first part of this Question is **yes**. However, it is my view that the exemptions have been correctly applied to the second part of this Question and I can confirm that the information that you are requesting regarding this is exempt by virtue of the following exemptions:

Section 24(1) – National Security
Section 31(1) – Law Enforcement

Both Sections 24 and 31 are prejudice based and qualified exemptions, therefore the harm (prejudice) in disclosure should be evidenced and the public interest given.

Overall Harm

Any disclosure under Freedom of Information is a release to the public at large. Whilst not questioning the motives of the requester, disclosure of a particular policing tool of this type being used by Wiltshire Police as part of an investigative process would reveal operational

Keeping Wiltshire Safe

tactics linked to policing, compromise police investigations and / or adversely affect the ability for us and others to safeguard national security.

It is well established that police forces utilise digital forensic techniques in order to counteract criminal behaviour, detect crime and assist in the apprehension and prosecution of offenders. Modern day policing is intelligence led and law enforcement depends upon the development of intelligence and the gathering and security of evidence in order to disrupt criminal behaviour and bring offenders to justice. As criminals adapt and exploit new technology, the police need to respond by overcoming hi-tech barriers in order to meet their responsibilities. In this case the information relates to a service provider and by extension their products for the extraction of data from devices to their kiosks.

By disclosing if Wiltshire Police use named software to process, analyse or evaluate data extracted from mobile phones such as requested within this FOI would undermine the process of preventing and detecting crime and the apprehension and prosecution of offenders. When considered on a force by force basis, a malign individual could identify and specifically target those most critical to the law and order sector. This would have a huge impact on the effective delivery of operational law enforcement as it would leave companies open to further cyberattacks which could have devastating consequences for law enforcement.

Equally, given the sensitive areas in which tools of this type may be used, such as counter-terror investigations, to disclose if any particular tools are used would allow criminals and other adversaries to focus on evaluating the particular capabilities of its use. With this knowledge it would allow criminals and other adversaries to take steps to counteract a specific tool – be it adjusting how they interact and present themselves to take advantage of any weaknesses or gaps in capability they identify. For example, at a simple level, if a policing tool doesn't search X social media site or was unable to identify Y format of images and criminals can establish this, they will exploit this position. Wiltshire Police's more sophisticated adversaries may be able to go further and take more proactive measures to undermine the tool and / or its provider and a specific confirmation allows efforts to be focused accordingly.

This detrimental effect is increased if the request is made to several different law enforcement bodies, which this request has been. 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 tools are or are not used. 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 Disclosure – Section 24

Disclosing would provide the public with information about technologies and police capabilities. This would reinforce the wider commitment to openness and transparency with the general public and facilitate public debate. Furthermore, owing to the inherent

Keeping Wiltshire Safe

link between transparency and public confidence, disclosing the software name and how it works would be likely to improve the general public's confidence in Wiltshire Police. Over time, an increase in public confidence would be likely to improve public engagement with the police. This would, in turn, lead to an improvement in our ability to both prevent and detect crime and apprehend and prosecute offenders.

Factors Favouring Non-Disclosure – Section 24

Security measures are put in place to protect the communities that we serve. To disclose the software name and its uses would be useful intelligence to terrorists and individuals intent on carrying out criminal activity. The public entrust the police service to make appropriate decisions with regards 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 those with ill intent gathering information about force capabilities would have greater impact when linked to other information gathered from various sources. The more information that is disclosed over time will provide a detailed account of the tactical infrastructure, not only at force level but across the country as a whole. Any incident that results from confirming that any information is held would by default, affect national security.

Factors Favouring Disclosure – Section 31

The public have a genuine interest in what the police do and how they do it. Their interest is legitimate and to be encouraged within a democratic society where policing is by consent. Public accountability for the use of resources and taxpayers' money, and a willingness to be open and transparent, are desirable characteristics in all public authorities. The interest on which software packages are being used and how is therefore to be expected, especially when there is some concern as to whether such expenditure is appropriate and justified.

Factors Favouring Non-Disclosure – Section 31

To disclose the particular software used and how it is used by Wiltshire Police would compromise our ability to protect the public. Disclosing Wiltshire Police's capabilities would provide persons intent on disrupting our work with information that would assist them to do so. In this case, for the reasons outlined in the evidenced harm, the effectiveness of current and future strategies when carrying out investigations and gathering evidence may be compromised. The safety of the public is of paramount importance to policing purposes and any increase in crime would place the public at risk of harm. When the current or future law enforcement role of Wiltshire Police may be compromised by the release of information, the effectiveness of Wiltshire Police will be reduced.

The personal safety of individuals is of paramount importance to the police service and must be considered in response of every release. A disclosure under Freedom of Information is a release to the world and, in this case, disclosing tactical information relating to the extraction of data from mobile devices would undermine the evidence gathering process of any investigative inquiry, including the most serious.

Balance Test

The above points highlight the merits of disclosure and non-disclosure. Having considered the reasons why Wiltshire Police should opt to not disclose the software name and its uses, although openness and transparency is at the forefront when considering the public

Keeping Wiltshire Safe

interest, in this case disclosing the software used and how it is analysed, evaluated and used by the police for investigative purposes would not be in the public interest.

Whilst there is a public interest in appropriately and effectively engaging with the threat from criminals, there is a very strong public interest in safeguarding national security. As much as there is a public interest in knowing that policing activity is appropriate and balanced in matters of national security, this will only be overridden in exceptional circumstances, which this Freedom of Information request is not.

The public entrust the police service to make appropriate decisions with regards to their safety and protection and the only way of reducing risk is to be cautious with any information that is released. Disclosing the software would reveal specific policing activity in the digital sphere of investigations and would assist those intent on causing harm. Any incident that results from disclosure would, as a result, affect national security.

It can be seen that disclosing the software used would directly harm the ability of Wiltshire Police to investigate crime. This could also reveal police capabilities, compromise police investigations and / or otherwise, adversely affect the ability of Wiltshire Police to safeguard national security. I have attached considerable weight to these interests as the primary role of the police service is to both prevent and detect crime and apprehend those responsible for committing criminal offences.

Therefore, at this moment in time, there is no public interest in disclosing information that would increase the risk to public safety and harm policing capabilities.

I am satisfied that all the relevant information has been passed to me and been considered in the light of your request within the time constraints applicable under the legislation.

Wiltshire Police would like to thank you for the interest that you have shown in the Force.

Yours Sincerely,

Wiltshire Police offers a re-examination of your case under its review procedure.



Force Disclosure Unit

Wiltshire Police HQ, London Road, Devizes, Wiltshire SN10 2DN



Freedom of Information Request Appeals Procedure

1. Who Can Ask for a Review

Any person who has requested information from Wiltshire Police, which has been dealt with under the Freedom of Information Act, is entitled to complain and request an internal review, if they are dissatisfied with the response they received.

2. How to Request a Review

Requests for review of a Freedom of Information request must be made in writing to the:

Force Disclosure Unit
Wiltshire Police Headquarters,
London Road, Devizes,
Wiltshire,
SN10 2DN

Email at disclosure@wiltshire.police.uk.

The reference number, date of the request and details of why the review is being requested must be included. Requests for review should be brought to the attention of the Force Disclosure Unit within 20 working days of the Force's response to the original Fol request.

3. Review Procedure

Receipt of a request for review will be acknowledged in writing to include confirmation of the reasons for the review. The review will be conducted by another Decision Maker, who is independent from the original Decision Maker. The Force Disclosure Unit will set a target date for a response. The response will be made as soon as is practicable with the intention to complete the review within twenty working days. In more complex cases the review may take up to 40 working days.

The Independent Decision Maker will conduct a review of the handling of the request for information and of decisions taken, including decisions taken about where the public interest lies in respect of exempt information where applicable. The review enables a re-evaluation of the case, taking into account the matters raised by the complaint.

4. Conclusion of the Appeal

On completion of the review the Independent Decision Maker will reply to the complainant with the result of the review. If the complainant is still dissatisfied following the review they should contact the Information Commissioner to make an appeal. The Information Commissioner can be contacted via the following details:

Keeping Wiltshire Safe

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 01625 545 700
Fax: 01625 524 510
Email: mail@ico.gsi.gov.uk

Please note that the ICO's offices will be closed for the foreseeable future and are therefore unable to receive correspondence via post.

If you should wish you contact them, please visit <https://ico.org.uk/global/contact-us/>