

8 April 2025

FOI Ref 17934

Request - You asked us the following:

Please confirm if your police force currently uses Cellebrite software. If so, please answer the following and provide copies of all:

1. Data Protection Impact Assessments directly related to Cellebrite software
2. Reports created in response to artificial intelligence services provided by Cellebrite
3. Guidance on data retention and information sharing as a result of information extracted by Cellebrite
4. Copies of all training and guidance provided to officers using Cellebrite
5. Please also provide figures on the following:
 - a. Since 01.01.23 until 01.03.25, how many times has Cellebrite been deployed by officers of your force, both:
 - i. Consensually
 - ii. Non-Consensually

We received your request on 10/03/2025 and have processed this under the Freedom of Information Act (FOIA).

Staffordshire Police's response to your enquiry is as follows:

Staffordshire Police can neither confirm nor deny whether information relevant to this request is held, as the duty in Section 1(1)(a) of the Freedom of Information Act 2000 does not apply by virtue of the following exemptions:

In accordance with Section 17(1) of the Freedom of Information Act, this letter represents a refusal notice for this particular request.

- Section 24(2) National Security
- Section 31(3) Law Enforcement

Section 24 and Section 31 are both qualified exemptions and as such there is a requirement to evidence any harm confirmation or denial that any other information is held as well as consider the public interest.

Harm

Any disclosure under FOI is a release to the public at large. Whilst not questioning the motives of the applicant, confirming or denying if a particular policing tool of this type (in this case Cellebrite products) is used by Staffordshire Police as part of an investigative process could reveal operational tactics linked to policing, compromise police investigations and/or adversely affect the ability of Staffordshire Police 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.

By revealing specific tactical information such as requested within this request, it would undermine the process of preventing or detecting crime and the apprehension of prosecution of offenders. When considered on a Force by Force basis, a malign individual could identify those most critical to the Law-and-Order sector and specifically target those proving the most assistance. 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.

Likewise, 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. Staffordshire 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. 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 deployed. 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 confirming or denying whether any information is held in respect of both exemptions claimed

Confirming or denying whether information is held in response to the request, would provide the public with information about technologies and Staffordshire 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 link between transparency and public confidence, confirming or denying whether information is held would be likely to improve the general public's confidence in Staffordshire 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 against confirming or denying whether any information is held for Section 24(2) - National Security

Security measures are put in place to protect the community that we serve. To confirm whether any information relevant to this request is/is not held would be useful intelligence to terrorists and individuals intent on carrying out criminal activity. Irrespective of what information is or is not 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 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 against confirming or denying whether any information is held for Section 31(3) - Law Enforcement

To confirm or deny information is held would compromise the forces' ability to protect the public. Disclosing Staffordshire Police capabilities would provide persons intent on disrupting their 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 the force may be compromised by the release of information, the effectiveness of the force 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 computers and other devices, would undermine the evidence gathering process of any investigative inquiry relating to offences, some of which may be serious cases such as murder or rape.

Balance Test

The points above highlight the merits of confirming, or denying, whether information relevant to this request does or does not exist. Having considered the reasons why Staffordshire Police should opt to neither confirm nor deny that information is held, although openness and transparency is at the forefront when considering the public interest, in this case confirmation or denial relating to Digital tools 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.

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 any information that is released. Confirming or denying whether information is or isn't held would reveal specific policing activity in the digital

sphere of investigations and would assist those intent on causing harm. Any incident that results from confirmation or denial could, as a result, affect National Security.

I have found that confirming or denying whether information is held in response to questions of this nature, would make public, areas of police interest. This would directly harm the ability of Staffordshire Police to investigate crime. This could also reveal police capabilities, compromise police investigations and/or otherwise, adversely affect the ability of Staffordshire 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, it is our opinion that for these issues the balance test for confirming, nor denying, that information is held is made out.

Freedom of Information Request Appeals Procedure

1. Who Can Ask for a Review

Any person who has requested information from Staffordshire 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 within two months of the date of receipt of this email, and should be addressed to:

foi@staffordshire.police.uk

Or by Post to:

Central Disclosure Unit
Staffordshire Police HQ
PO Box 3167
Stafford
ST16 9JZ

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 Central Disclosure Unit within two months of the Force's response to the original FOI request.

3. Review Procedure

Receipt of a request for review will be acknowledged in writing. The review will be conducted by another Decision Maker who is independent from the original Decision Maker. The Central 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 20 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



STAFFORDSHIRE
POLICE

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:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ICO Website for complaints link: <https://ico.org.uk/make-a-complaint/foi-and-eir-complaints/foi-and-eir-complaints/>

Freedom of Information
Central Disclosure Unit