

10 December 2024

FOI Ref 17465

Request - You asked us the following:

I'm writing to you under the Freedom of Information Act (2000) to ask if you currently, or at any point in the last 5 years, have or hold a contract with the company Palantir Technologies.

I'll note for the purposes of transparency declarations under the act that this information would not be covered by National Security or law enforcement exemptions, as a recent contract with Leicestershire police has recently been made public voluntarily through the government's contracts finder website, the details of which are here below:

<https://www.contractsfinder.service.gov.uk/notice/ce565f22-d758-4294-bf2d-62e3129063a2?origin=SearchResults&p=1>

I'd like to know the cost if applicable, as well as the timeframe of the contract, a vague outline of the work (if this can be made available), and if this has the option to extend or not.

I'd like to know as well, if the force has met with Palantir at any point over the last two years to discuss future contracts, if so, can I have the minutes of these meetings please.

We received your request on 14/11/2024 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 24(2) is a qualified exemption and as such there is a requirement to articulate the harm and conduct a test of the public interest in confirmation or denial.

- Section 31(3) - Law Enforcement.

Section 31(3) is a qualified exemption and as such there is a requirement to articulate the harm and conduct a test of the public interest in confirmation or denial.

Public Interest Test

Harm in confirming or denying that information is held

Any disclosure under FOI is a release to the public at large. Whilst not questioning the motives of the applicant, confirming or denying that any other information relating to the covert software and its uses would show criminals what the capacity, tactical abilities and capabilities of the force are, allowing them to target specific areas of the UK to conduct their criminal/terrorist activities. Confirming or denying the specific circumstances in which the Police Service may or may not deploy the use of covert software would lead to an increase of harm to covert investigations and compromise law enforcement. This would be to the detriment of providing an efficient policing service and a failure in providing a duty of care to all members of the public.

The threat from terrorism cannot be ignored. It is generally recognised that the international security landscape is increasingly complex and unpredictable. Since 2006, the UK Government has published the threat level, based upon current intelligence and that threat is currently categorised as SUBSTANTIAL.

The UK continues to face a sustained threat from violent extremists and terrorists. It is well established that police forces use covert tactics and surveillance to gain intelligence in order to counteract criminal behaviour. It has been previously documented in the media that many terrorist incidents have been thwarted due to intelligence gained by these means.

Confirming or denying whether any information is or isn't held relating to the covert software offered by specific companies would limit operational capabilities as criminals/terrorists would gain a greater understanding of the police's methods and techniques, enabling offenders to take steps to counter them. It may also suggest the limitations of police capabilities in this area, which may further encourage criminal/terrorist activity by exposing potential vulnerabilities. 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 tactics 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.

Staffordshire Police needs to be alert to requests for certain types of information, and there is a need for consistency when neither confirming nor denying whether information is held in order to protect policing information.

Factors in favour of disclosure

Confirming or denying whether the requested information is held would enable the public to have a better understanding of the type of policing tools and tactics employed by Staffordshire Police in carrying out their law enforcement role. This would give more confidence to the public that we are using (or, as the case may be, not using) policing tools and tactics to help us detect and prevent crime appropriately.

Factors against disclosure

To confirm or deny whether any other information relating to the use of a particular investigative tool is held would harm the integrity of sensitive policing tactics used to prevent and detect crime and safeguard national security.

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 Palantir Technologies) is used by Staffordshire Police as part of an investigative process is different from confirming if, in principle, commercial tools generally are used to assist with searches against information that may be found online.

It is well established that police forces use publically available data in order to counteract criminal behaviour. It has been previously documented in the media that many terrorist incidents have been thwarted due to intelligence gained by these means. However, given the sensitive areas in which tools of this type may be used and Staffordshire Police's role in 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 a particular tool. 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. 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.

Balance Test

Accordingly, in a position taken in common with other law enforcement agencies, confirming or denying if Staffordshire Police uses Palantir Technologies would lead to an increase of harm to covert investigations and compromise law enforcement. This outweighs the benefits to disclosure, not least as disclosure would be to the detriment of providing an efficient policing service and a failure in providing a duty of care to all members of the public. Therefore it is our opinion that for these issues the balance test favours neither confirming nor denying that information is held.

If it exists, the disclosure of this information to the public by Staffordshire Police would undermine the integrity of police investigations and operations and in maintaining confidence in Staffordshire Police.

The effective delivery of operational law enforcement is of paramount importance to Staffordshire Police in their duty to ensure that the prevention and detection of crime is carried out and the effective apprehension or prosecution of offenders is maintained.

Therefore it is our opinion that for these issues the balance test favours neither confirming nor denying that information is held.

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 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



STAFFORDSHIRE
POLICE

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