

From: [NPCC CRU Mailbox](#)
Subject: Update to - RE: Log No.995/24 CRU Circulation (12/11/2024) - **S38(1)(b)** - Palantir - OS
Date: 09 December 2024 14:45:09
Attachments: [image001.png](#)
[image002.png](#)
[IR Advice Log No.00175022 CRU Circulation \(29112022\) .msq](#)

OFFICIAL - SENSITIVE
POLICE EYES ONLY

Not to be distributed outside of the Police network or other agencies without prior authorisation from the CRU

Dear All,

Apologies for having to wait and chase on this one. The decision taken is to continue the stance previously given in 2022 which we also held at IR stage (CRU 1750/22 – **S38(1)(b)** refers). Whilst applicant and motive blind I think it is reasonable to suggest that the link **S30(c) & S38(1)(b), S35(1)(a)&(b)**

[REDACTED]

In brief, the continued approach is :

- if your force has placed a formal disclosure regarding the use of Palantir technology into the public domain then you can confirm information is held and exempt it via s21, providing a link to the information in the public domain. A partial NCND s31(3) and s24(2) will also be required for any information that may or may not be held in relation to Palantir software used for covert purposes..
- If your force has not formally acknowledged use of Palantir software then a full NCND is required via s31(3) and s24(2).

I have attached the previous advice and IR advice for 1750/22 which gives further explanation as to the rationale for the decision.

In addition, a form of words kindly supplied by the MPS is below to assist. Reference to the MPS needs to be removed and replaced accordingly.

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

Section 1 of the Act places two duties on public authorities. Unless exemptions apply, the first duty at Section 1(1)(a) is to confirm or deny whether the information specified in a request is held. The second duty at Section 1(1)(b) is to disclose information that has been confirmed as being held. Where exemptions are relied upon Section 17 of the Act requires that we provide the applicant with a notice which: a) states that fact; b) specifies the exemption(s) in question and c) states (if that would not otherwise be apparent) why the exemption(s) apply.

The MPS 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 the MPS 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 the Met 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 the Met'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. The Met'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.

Balancing test

Accordingly, in a position taken in common with other law enforcement agencies, confirming or denying if the Met 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 the MPS would undermine the integrity of police investigations and operations and in maintaining confidence in the MPS.

The effective delivery of operational law enforcement is of paramount importance to the MPS 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.

Kind regards,

S38(1)(b)

Freedom of Information Referral Officer
National Police Freedom of Information and Data Protection Unit
National Police Chiefs Council

NPFDU PO Box 481, Fareham, Hampshire. PO14 9FS

 **S30(c) & S38(1)(b)** [@npfd.police.uk](mailto:npfd@npfd.police.uk)

S30(c) & S38(1)(b), S30(1)(a)(i)



From: NPCC CRU Mailbox
Sent: 12 November 2024 10:26
Subject: Log No.995/24 CRU Circulation (12/11/2024) - S38(1)(b) - Palantir - OS

OFFICIAL - SENSITIVE
POLICE EYES ONLY

Not to be distributed outside of the Police network or other agencies without prior authorisation from the CRU

Dear All,

The following FOI request has been logged in the CRU today - **Please let us know if you have received it.**

The applicant submitted a similar request to the majority of forces in 2022 – CRU ref 1750/22. However, before re-issuing the same advice I will carry out a review with relevant policing leads. Advice will follow in due course.

Log Number:995/24
Case worker: S38(1)(b)
Logged with:Cambridgeshire Constabulary
Sent from: S38(1)(b)

Applicants Request

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:

[NECTAR - EMSOU - Contracts Finder](#)

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.

Kind regards,

S38(1)(b)
Freedom of Information Referral Officer
National Police Freedom of Information and Data Protection Unit
National Police Chiefs Council
NPFDU PO Box 481, Fareham, Hampshire. PO14 9FS
S30(c) & S38(1)(b) @npfdu.police.uk
S30(c) & S38(1)(b)



This email contains information which is confidential and may also be privileged. It is for the exclusive use of the addressee(s) and any views or opinions expressed within are those of the originator and not necessarily those of the Force. If you are not the intended recipient(s) please note that any form of distribution, copying or use of this email or the information contained is strictly prohibited and may be unlawful. If you have received this communication in error please forward a copy to informationsecurity@thamesvalley.police.uk and to the sender. Please then delete the email and destroy any copies of it. DO NOT use this email address for other enquiries as it will not be responded to, nor any action taken upon it. If you have a non-urgent enquiry, please call the Police non-emergency number 101. If it is an emergency, please call 999. Thank you.

From: [NPCC CRU Mailbox](#)
Subject: Log No.157/25 CRU Circulation (21/03/2025) - Including Advice
Date: 25 March 2025 10:09:07
Attachments: [image001.png](#)
[image002.png](#)
[Update to - RE Log No.99524 CRU Circulation \(12112024\) - - Palantir - OS.msg](#)

OFFICIAL – SENSITIVE

POLICE EYES ONLY

Not to be distributed outside of the Police network or other agencies without prior authorisation from the CRU

Dear All,

Please see below advice in relation to the following:

Log Number:157/25
Logged with: National

Applicants Request

I'm seeking copies of any and all of the following documents in relation to your organisation's use of services provided by Palantir Technologies UK Ltd.

A list of current and past contracts, with start and end dates (where applicable) Any and all Data Processing Arrangements Any and all Data Sharing Agreements Any and all Data Protection Impact Assessments

I note that many UK police forces have previously declined to confirm or deny the existence of information relating to Palantir. However, police forces including Bedfordshire and Leicestershire have since publicly confirmed using the company's services, setting a precedent for disclosure.

Additionally, Palantir is a well-known provider of products that rely on artificial intelligence. The NPCC's Covenant for Using Artificial Intelligence in Policing, endorsed by all UK police forces, states that "all use of AI will be subject to 'Maximum Transparency by Default'".

CRU Advice

Practitioners may recall the advice to maintain NCND for CRU 995/24 (attached). The same advice is still in play now.

In short, it is the need for consistency in response as to when FOI is used to work out exactly what products or tools are being used, and by which forces.

Kind regards,

S38(1)(b)

Freedom of Information Referral Officer
National Police Freedom of Information and Data Protection Unit
National Police Chiefs Council

NPFDU PO Box 481, Fareham, Hampshire. PO14 9FS

 npfd@npfd.police.uk

S30(C) & S38(1)(b), S30(1)(d)&(e)



This email contains information which is confidential and may also be privileged. It is for the exclusive use of the addressee(s) and any views or opinions expressed within are those of the originator and not necessarily those of the Force. If you are not the intended recipient(s) please note that any form of distribution, copying or use of this email or the information contained is strictly prohibited and may be unlawful. If you have received this communication in error please forward a copy to informationsecurity@thamesvalley.police.uk and to the sender. Please then delete the email and destroy any copies of it. DO NOT use this email address for other enquiries as it will not be responded to, nor any action taken upon it. If you have a non-urgent enquiry, please call the Police non-emergency number 101. If it is an emergency, please call 999. Thank you.
