



Your reference: N/A

Our reference: FOI_25_0193

E-mail: FOI
@gloucestershire.police.uk

Direct dial: 01452 754304

Postal Address: As above

Date: 28/03/2025

Dear

Gloucestershire Constabulary Freedom of Information request FOI_25_0193

On 13/02/2025 you sent an email constituting a request under the Freedom of Information Act asking the following:

Please accept this request under the Freedom of Information Act. 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'".

In order to provide you with a response, further enquiries were needed, therefore a PIT Extension was applied on 13/03/2025.

Section 1 of the Freedom of Information Act 2000 (FOIA) 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 s17 of FOIA 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 applies.

Gloucestershire Constabulary can neither confirm nor deny that it holds any information in relation to systems used for intelligence purposes as the duty in Section 1(1)(a) of the Freedom of Information Act 2000 does not apply, by virtue of the following exemptions:

Section 24(2) National Security
Section 31(3) Law enforcement;

Section 24 and 31 are prejudice based qualified exemptions and there is a requirement to articulate the harm that would be caused in confirming or not that the information is held as well as carrying out a public interest test.

Harm

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 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.

Public Interest Test

Factors favouring confirming or denying information exists

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 Gloucestershire Constabulary 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 confirming or denying information exists

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 Gloucestershire Constabulary 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 Gloucestershire Constabulary 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. Gloucestershire Constabulary 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 Gloucestershire Constabulary 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 Gloucestershire Constabulary would undermine the integrity of police investigations and operations and in maintaining confidence in Gloucestershire Constabulary.

The effective delivery of operational law enforcement is of paramount importance to Gloucestershire Constabulary 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.

If you are not satisfied with this response or any actions taken in dealing with your request, you have the right to ask that we review your case under our internal procedure. Please note that a request for an internal review must be made within 20 working days of the response to your original request.

If you decide to request that such a review is undertaken and following this process you are still unsatisfied, you then have the right to direct your complaint to the Information Commissioner for consideration.

The Information Commissioner can be contacted via the following means:

Website - <https://ico.org.uk/>

Call their helpline - 0303 123 1113

Email - casework@ico.org.uk

Post –

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

Yours sincerely,

Disclosure Officer

