



Your reference: N/A
Our reference: FOI_24_1018
E-mail: FOI
@gloucestershire.police.uk
Direct dial: 01452 754304
Postal Address: As above
Date: 11/12/2024

Dear

Gloucestershire Constabulary Freedom of Information request FOI_24_1018

On 13/11/2024 you sent an email constituting a request under the Freedom of Information Act asking the following:

Dear Gloucestershire Constabulary

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.

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 (s24)

The public are entitled to know how public funds are spent and how resources are distributed within an area of policing. To confirm or deny that Gloucestershire Constabulary uses specific software would enable the general public to hold to account forces who use out of date software. In the current financial climate of cuts and with the call for transparency of public spending this would enable improved public debate into this subject.

Factors against confirming or denying information exists (s24)

Security measures are put in place to protect the community we serve. As evidenced within the harm, to confirm or deny that any information is held would highlight to terrorists and individuals intent on carrying out criminal activity vulnerabilities within the operating systems of Gloucestershire Constabulary.

Taking into account the current security climate within the United Kingdom, the Constabulary should not confirm or deny information is held which may aid a terrorist. To what extent this information may aid a terrorist is unknown, but it is clear that it will have an impact on a force's ability to monitor terrorist activity. 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. Any incident that results from such a disclosure would, by default, affect National Security.

Factors favouring confirming or denying information exists (s31)

Confirming that information exists or not relevant to this request would lead to a better informed public which may encourage individuals to provide intelligence in order to reduce the risk of police networks being hacked.

Factors against confirming or denying information exists (s31)

Disclosing whether information is or is not held relevant to your request would show that Gloucestershire Constabulary take their responsibility to protect information and information systems from unauthorised access, destruction, etc., dismissively and inappropriately.

Balancing Test

The Police Service is charged with enforcing the law, preventing and detecting crime and protecting the communities we serve. As part of that policing purpose, information is gathered which can be highly sensitive relating to high profile investigative activity.

Weakening the mechanisms used to monitor any type of criminal activity, and specifically terrorist activity by confirming or denying information relevant to your request is held, would place the security of the country at an increased level of danger.

In order to comply with statutory requirements and to meet NPCC expectation of the Police Service with regard to the management of information security a national policy approved by the College of Policing titled National Policing Community Security Policy has been put in place. This policy has been constructed to ensure the delivery of core operational policing by providing appropriate and consistent protection for the information assets of member organisations.

Anything that places that confidence at risk, no matter how generic, would undermine any trust or confidence individuals have in the Police Service. It is therefore our opinion that for these issues the balancing test for confirming or denying that information is held is not made out.

No inference can be drawn from these facts that any information does or does not exist. 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
Gloucestershire Constabulary