

**Force Disclosure Unit**

Wiltshire Police HQ

London Road

Devizes

Wiltshire

SN10 2DN

Tel 101 ext. 62005

[www.wiltshire.police.uk](http://www.wiltshire.police.uk)[disclosure@wiltshire.police.uk](mailto:disclosure@wiltshire.police.uk)

Date: 20 May 2022

Our ref: FOI 2022/307

Reply contact name is: Lloyd Tilbury

Dear,

I write in connection with your request for information dated 6<sup>th</sup> April 2022.

I am required by the Freedom of Information Act 2000 to handle all requests in a manner that is blind as to the identity and motives of the requestor. Any information released as a response to a request is regarded as being published and therefore in the public domain without caveat.

Your request for information has now been considered and I am able to respond as follows.

**You wrote:**

I'm writing to you under the Freedom of Information Act (2000) to ask that you please disclose to me whether your force uses the company DATAMINR.

I'd like to know of any contract that you hold with this company, from 2019 to present, or, if not direct contracts, whether or not you use this company / have bought it through a third party software broker.

I'd like to know, if the previous answer is yes, what events it has tracked for you, including any and all protest events, and who's tweets / which news events were targeted by it, including BLM, XR, Insulate Britain, Women's Marches, "antifa", anti-arms trade groups, trade unions, environmentalist groups, or LGBTQ+ rights campaigners.

I'd also like a copy of the contract, if relevant, and user service agreement for this work.

Dataminr have been found in the past to facilitate domestic surveillance of peaceful protests, not only of activists but of bystanders, both at the behest of law enforcement officials and intelligence services, by accessing the twitter firehose service and feeding information directly back to these bodies. This violated twitter policy, and resulted in twitter kicking the CIA off of the service as far back as 2016, after which point dataminr were found to be engaging in the same activity again in 2020, after having lied about doing so, by monitoring BLM protestors in the wake of the murder of George Floyd.



INVESTOR IN PEOPLE

The public have a right to know when domestic surveillance is being carried out, both by a public body but specifically a third party with a questionable track record operating on behalf of said public body, and there deserves to be a free and focused discourse as to the methods law enforcement use in order to enact public safety. It is for this reason that I have to request that you re-examine the response given to me here, and provide me with the information I'm requesting.

### **Response:**

On reviewing your original request, the response provided to you and your request for an Internal Review, I uphold the original response provided to you.

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

Section 24(2) – National Security

Section 31(3) – Law Enforcement

### **Overall Harm in Confirming or Denying whether Information is Held**

Any disclosure under Freedom of Information is a release to the public at large. Under the Act, we cannot, and do not request the motives of any application for information. We have no doubt that the vast majority of requests made under the Act are legitimate and the applicants do not have ulterior motives. Whilst not questioning the motives behind this specific request, confirming or denying that information is held regarding business with DATAMINR, or any other likeminded third-party provider, would cause operational harm and affect our ability to fulfil our core function of law enforcement in the future. Confirming or denying whether or not information is held would allow members of the public to identify the resources and tactics used to identify and respond to emergency operations such as widespread disorder, protests, demonstrations, wide scale disasters etc... It would enable individuals and organisations that are intent on causing disruption to identify strengths and weaknesses at force level, and more so nationally, which could be exploited causing harm to members of the public.

In addition, confirming or denying the specific circumstances in which the Police Service may or may not deploy tools described as capable of gathering intelligence from the internet, would likely 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 judged as "substantial", meaning that an attack on the UK is likely. It is well established that police forces use tactics and technology to gain intelligence in order to counteract criminal behaviour, and 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 held about the use of internet intelligence gathering tools/platforms 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 disrupting policing functions throughout the UK will be able to 'map' where the use of certain

tactics may or may not be deployed. This can be useful information to those committing (or those intent on committing or planning) crime.

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**

#### **Section 24(2) – National Security**

##### **Factors Favouring Confirming or Denying that Information is Held**

The information, if held, only relates to national security and confirming or denying whether it is held would not actually harm it. The public are entitled to know what public funds are spent on and what measures are in place. By confirming or denying if business is conducted with DATAMINR, or any other likeminded third-party provider, it would lead to a better-informed public.

##### **Factors Against Confirming or Denying that Information is Held**

By confirming or denying whether any information is held would render policing and security measures less effective. This would lead to the compromise of ongoing or future operations to protect the security or infrastructure of the UK and increase the risk of harm to the public.

#### **Section 31(3) – Law Enforcement**

##### **Factors Favouring Confirming or Denying that Information is Held**

Confirming or denying whether business is conducted with DATAMINR, or any other likeminded third-party provider, would provide an insight into the Police Service. This would enable the public to have a better understanding of the effectiveness of the police and about how the police gather intelligence. It would greatly assist in the quality and accuracy of public debate, which could otherwise be steeped in rumour and speculation. Where public funds are being spent, there is a public interest in accountability and justifying the use of public money.

##### **Factors Against Confirming or Denying that Information is Held**

Confirming or denying that any information is held regarding business with DATMINR, or any other likeminded third-party provider, would have the effect of compromising law enforcement tactics. It has been recorded that Freedom of Information releases are monitored by criminals and terrorists and so to confirm or deny information is held concerning intelligence gathering would lead to law enforcement being undermined. The Police Service is reliant upon all manner of techniques during operations and the public release of any modus operandi employed, if held, would prejudice the ability of the Police Service to perform the functions it exists to provide.

By confirming or denying that a business interest exists would hinder the prevention and detection of crime. The Police Service would not wish to reveal what tactics may or may not have been used to gain intelligence as this would clearly undermine the law enforcement and investigative process. This would impact on police resources and more crime and terrorist incidents would be committed, placing individuals at risk. It can be argued that there are significant risks associated with providing information, if held, in relation to any aspect of investigations or of any nation's security arrangements so confirming or denying that information is held, may reveal the relative vulnerability of what we may be trying to protect.

## **Balance Test**

The security of the country is of paramount importance and Wiltshire Police will not divulge whether any information is or is not held regarding business with any company, if to do so would place the safety of an individual at risk, undermine National Security or compromise law enforcement.

Whilst there is a public interest in the transparency of policing operations and providing assurance that Wiltshire Police is appropriately and effectively engaging with the threat posed by various groups or individuals, there is a very strong public interest in safeguarding the integrity of police investigations and all areas of operations carried out by police forces throughout the UK.

As much as there is public interest in knowing that policing activity is appropriate and balanced this will only be overridden in exceptional circumstances. The use of technology can be a sensitive issue that would reveal police tactics and therefore it is our opinion that for these issues the balancing test for confirming or denying whether any information is held regarding the police, DATAMINR, or any other likeminded third-party provider, is not made out.

However, this should not be taken as necessarily indicating that any information that would meet your request exists or does not exist.

I am satisfied that all the relevant information has been passed to me and been considered in the light of your request within the time constraints applicable under the legislation.

Wiltshire Police would like to thank you for the interest that you have shown in the Force.

Yours sincerely,

**Lloyd Tilbury**  
**Principal Decision Maker**

Wiltshire Police offers a re-examination of your case under its review procedure.



## **Force Disclosure Unit**

Wiltshire Police HQ, London Road, Devizes, Wiltshire SN10 2DN  
Telephone 101 ext 62005

### **Freedom of Information Request Appeals Procedure**

#### **1. Who Can Ask for a Review**

Any person who has requested information from Wiltshire 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 to the:  
Force Disclosure Unit  
Wiltshire Police Headquarters,  
London Road, Devizes,  
Wiltshire,  
SN10 2DN

Email at [disclosure@wiltshire.police.uk](mailto:disclosure@wiltshire.police.uk).

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 Force Disclosure Unit within 20 working days of the Force's response to the original FoI request.

#### **3. Review Procedure**

Receipt of a request for review will be acknowledged in writing to include confirmation of the reasons for the review. The review will be conducted by another Decision Maker, who is independent from the original Decision Maker. The Force 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 twenty 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 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  
Tel: 01625 545 700  
Fax: 01625 524 510  
Email: [mail@ico.gsi.gov.uk](mailto:mail@ico.gsi.gov.uk)

**Please note that the ICO's offices will be closed for the foreseeable future and are therefore unable to receive correspondence via post.**

**If you should wish you contact them, please visit <https://ico.org.uk/global/contact-us/>**