Freedom of Information Act 2000 (FOIA)

Decision notice

Date: **13 December 2022**

Public Authority: **Chief Constable of South Yorkshire Police**
Address: **South Yorkshire Police Headquarters**
Carbrook House
Carbrook Hall Road
Sheffield
S9 2EH

Decision

1. The complainant has requested information relating to South Yorkshire Police's (SYP) relationship with the company 'Dataminr' (a real time AI platform that detects the earliest signals of high-impact events emerging risks from within publicly available data.)

2. The Commissioner's decision is that the Home Office was entitled to refuse to comply with the request in accordance with section 24(2). No steps are required.

Request and response

3. On 28 July 2021 the complainant requested information of the following description:

> "1. 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.
>
> 2. 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.

3. 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.

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

4. SYP responded neither confirming nor denying whether it held the information citing section 24(2) and section 31(3) of the FOIA.

Reasons for decision

Neither confirm nor deny ("NCND")

5. Section 1(1)(a) of FOIA requires a public authority to inform a requester whether it holds the information specified in the request. However, there may be occasions when complying with the duty to confirm or deny under section 1(1)(a) would in itself disclose sensitive or potentially damaging information that falls under an exemption. In these circumstances, FOIA allows a public authority to respond by refusing to confirm or deny whether it holds the requested information.

6. The decision to use a neither confirm nor deny response will not be affected by whether a public authority does, or does not, hold the requested information. The starting point, and main focus in most cases, will be theoretical considerations about the consequences of confirming or denying whether or not a particular type of information is held.

7. It is sufficient to demonstrate that either a hypothetical confirmation, or a denial, would engage the exemption. In other words, it is not necessary to show that both confirming and denying information is held would engage the exemption from complying with section 1(1)(a) of FOIA.

8. In this case, SYP argued that it is not obliged to provide confirmation or denial as to whether it holds the requested information by virtue of two exemptions which it considers apply, section 24(2) and section 31(3).

9. The Commissioner is mindful that the decision to neither confirm nor deny is separate from a decision not to disclose information and needs to be taken entirely on its own merits.

10. The Commissioner has first considered SYP's application of section 24(2).

Section 24 - National security

11. Section 24(2) provides an exemption from the duty to confirm or deny where this is required for the purpose of safeguarding national security.

12. FOIA does not define the term national security. However, in Norman Baker v the Information Commissioner and the Cabinet Office (EA/2006/0045 4 April 2007) the Information Tribunal was guided by a House of Lords case (Secretary of State for the Home Department v Rehman [2001] UKHL 47) concerning whether the risk posed by a foreign national provided grounds for his deportation. The Information Tribunal summarised the Lords' observations as follows:

    • 'national security' means the security of the United Kingdom and its people;

    • the interests of national security are not limited to actions by an individual which are targeted at the UK, its system of government or its people;

    • the protection of democracy and the legal and constitutional systems of the state are part of national security as well as military defence;

    • action against a foreign state may be capable indirectly of affecting the security of the UK; and,

    • reciprocal co-operation between the UK and other states in combating international terrorism is capable of promoting the United Kingdom's national security.

13. The approach that the Commissioner takes to the term 'required' as it is used in this exemption is that this means 'reasonably necessary.' In effect, this means that there has to be a risk of harm to national security for the exemption to be relied upon, but there is no need for a public authority to prove that there is a specific, direct, or imminent threat.

14. Therefore, section 24(2) is engaged if the exemption from the duty to confirm or deny is reasonably necessary for the purpose of safeguarding national security. The Commissioner considers that section 24(2) should be interpreted so that it is only necessary for a public authority to show that either a confirmation or a denial of whether requested information is held would be likely to harm national security. It is not necessary to show that harm would flow from both.

15. SYP explained that disclosing information about any relationship it may or may not have with the company 'DATAMINR' 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, terrorist incidents, wide scale disasters etc. In addition, SYP argued that it would enable individuals and organisations who are intent on causing disruption to identify strengths and weaknesses at force level, and more so nationally, which could be exploited in order to harm members of the public, or local or national infrastructure.

16. SYP argued that the threat from terrorism cannot be ignored and it is generally recognised that the international security landscape is increasingly complex and unpredictable. It stated that 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.

17. SYP also argued that 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. It also explained that it is well known that FOIA releases are monitored by criminals and terrorists and so to confirm or deny information is held concerning specific methods of intelligence gathering would risk national security.

18. SYP stated that by 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 explained that it may also suggest the limitations of police capabilities in this area, which may further encourage criminal/terrorist activity by exposing potential vulnerabilities.

19. SYP argued that this detrimental effect is increased if the request is made to several different law enforcement bodies and 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. It stated that this can be useful information to those committing (or those intent on committing or planning) crime.

20. SYP concluded that 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.

21. The Commissioner accepts that this reasoning is relevant to section 24; by confirming or denying whether the information is held would potentially disclose to terrorist individuals or organisations which forces use intelligent gathering software.

22. The Commissioner recognises, for example, that terrorists can be highly motivated and may go to great lengths to gather intelligence. He acknowledges that gathering information from publicly available sources, in this case responses from other forces, may be a strategy used by those planning terrorist activities.

23. The next step is to consider whether there would be a causal link between disclosure of the information in question and the predicted outcome of undermining the ability of SYP to provide effective protection. This could be, for example, by worsening or extending the threat of a terrorist attack. The Commissioner accepts that there is a reasonable likelihood of there being individuals or groups who would seek to exploit this information.

24. SYP has explained that 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.

25. The Commissioner recognises that the routine confirmation or denial of whether forces use intelligent gathering software would identify strengths and weaknesses amongst forces as it would provide information which would help those concerned to gauge the extent to which they might have evade detection.

26. In reaching his conclusion in this case, the Commissioner does not dispute the very real risks which exist around the security of the nation. It follows that, when considering the application of section 24, the Commissioner recognises that there may be grounds for issuing a NCND response in respect of what, on the face of it, appears to be harmless information. For example, it may be necessary to NCND holding information on the basis that confirmation (or otherwise) of its existence it may assist terrorists or lone individuals when pieced together with other information they may obtain from other sources. In this case as the request has been made to multiple forces, there is a potential to identify which forces have weaker detection capabilities, therefore were

an attack planned, it may have wider safety implications for the general public.

27. In view of the above, the Commissioner finds that it is reasonably necessary for the purpose of national security for SYP to NCND whether or not the requested information is held. His conclusion is, therefore, that the exemption provided by section 24(2) of FOIA is engaged. The Commissioner has therefore gone on to consider the public interest in neither confirming nor denying that the requested information is held.

Public interest for confirming or denying

28. SYP stated that it always strive to be as transparent as possible as we believe that the public are entitled to know how the police operates, how we are keeping the public safe and how we are spending their public money.

29. It explained that confirming whether it has a relationship with 'Dataminr' would enable the public to have a better understanding of the effectiveness of the police and about how forces gather intelligence. It may also 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 justification of the use of public money.

30. It added that confirming whether it has a relationship with 'Dataminr' would fulfil its aspiration of transparency.

31. In his request for internal review the complainant raised the following:

> "'Dataminr' have been known 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 those bodies. He explained that 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, monitoring BLM protestors in the wake of the murder of George Floyd."

32. The complainant argued that the public have a right to know when domestic surveillance is being carried out, both by a public body but specifically a third party operating on behalf of said public body, and there deserves to be a free and focused discourse as to the methods law enforcement agencies use in order to enact public safety.

Public interest against confirming or denying

33. SYP argued that it is well known that FOIA releases are monitored by criminals and terrorists and so to confirm or deny information is held concerning intelligence gathering would lead to national security being undermined.

34. SYP also argued 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 infra-structure of the UK and increase the risk of harm to the public.

35. SYP stated that if it becomes publicly known that SYP or other forces may use 'Dataminr', they could be specifically targeted in order to disrupt police operations at a particular time to coincide with criminal or terrorist activity, in order to specifically prevent the police's ability to secure and safeguard the public.

Balance of the public interest

36. The Commissioner recognises that there are some valid public interest arguments in confirmation or denial in response to this request brought forward by the complainant. The Commissioner agrees that it would increase public knowledge and assist in the quality and accuracy of public debate in regards to police forces using third party companies who gather intelligence via social media platforms.

37. Although the Commissioner understands and recognises the points raised by the complainant, the Commissioner must recognise the public interest inherent in this exemption. Safeguarding national security is a matter of the most fundamental public interest; its weight can be matched only where there are also fundamental public interests in favour of confirmation that the requested information is held.

38. As the request has been made to multiple police forces, the Commissioner recognises that if SYP was to confirm or deny whether the information requested was held, this could reveal which forces have stronger intelligence gathering capabilities and could therefore expose vulnerabilities between forces, this could then be taken advantage of by terrorists or organisations and, as a result jeopardise the national security of the UK and its citizens.

39. The Commissioner agrees with SYP that there the public interest lies in ensuring that the national security of the UK is not compromised and given the risks of complying with section 1(1)(a), he has therefore concluded that the public interest favours maintaining the exemption contained at section 24(2) of FOIA.

40. In light of this finding the Commissioner has not considered the SYP's reliance on section 31(3) of FOIA.

Right of appeal

41. Either party has the right to appeal against this decision notice to the First-tier Tribunal (Information Rights). Information about the appeals process may be obtained from:

    First-tier Tribunal (Information Rights)
    GRC & GRP Tribunals,
    PO Box 9300,
    LEICESTER,
    LE1 8DJ

    Tel: 0203 936 8963
    Fax: 0870 739 5836
    Email: grc@justice.gov.uk
    Website: www.justice.gov.uk/tribunals/general-regulatory-chamber

42. If you wish to appeal against a decision notice, you can obtain information on how to appeal along with the relevant forms from the Information Tribunal website.

43. Any Notice of Appeal should be served on the Tribunal within 28 (calendar) days of the date on which this decision notice is sent.

Signed .....

Laura Tomkinson
Group Manager
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF