

Freedom of Information Act 2000 (FOIA)

Decision notice

Date: 23 March 2023

Public Authority: Cabinet Office

Address: 70 Whitehall
London
SW1A 2AS

Decision (including any steps ordered)

1. The complainant made a two-part request for information about use of software supplied by Dataminr. The above public authority ("the public authority") relied on sections 41 (breach of confidence) and 43 of FOIA (commercial interests) to withhold information within the scope of part 1 and a number of exemptions to withhold information within the scope of part 2.
2. The Commissioner's decision is that the public authority is entitled to rely on section 43 of FOIA to withhold the information within the scope of part 1 of the request and that the balance of the public interest favours maintaining that exemption. In relation to part 2, some of the withheld information engages section 23 (security bodies) of FOIA. The remainder engages section 24 (national security) of FOIA and the balance of the public interest favours maintaining this exemption. The Cabinet Office breached section 17 of FOIA in dealing with this request because it took an unreasonable amount of time to consider the balance of the public interest.
3. The Commissioner does not require further steps to be taken.

Request and response

4. On 7 January 2022, the complainant wrote to the public authority and requested information in the following terms:

"[1] I'm writing to you under the Freedom of Information Act (2000) to ask that you please disclose the user manual and any training documents given to the department when it undertook licences with the company DATAMINR...

"[2] I'd also like to know what topics, or themes, since it has been in operation, that DATAMINR has provided the CO with 'situational awareness' over. I'd like this information in full please, as in, for covid response, protest monitoring, supply chain, or and all other application of the product since the contract was undertaken."

5. The public authority responded on 28 June 2022. In relation to element [1], it relied on sections 43 and 41 of FOIA (breach of confidence) to withhold the information. In respect of element [2], the Cabinet Office cited six exemptions including section 23 (security bodies) and section 24 (national security) of FOIA.
6. Following an internal review the public authority upheld its previous stance.

Reasons for decision

Part 1 – commercial interests

7. The information falling within the scope of this part of the request is a short technical guide advising how the software can be used to produce a desired outcome.
8. Section 43 of FOIA allows a public authority to withhold information whose disclosure would, or would be likely to, prejudice either its own commercial interests or those of another party.
9. The public authority explained that it had consulted Dataminr which had confirmed that, in its view, disclosure of the document would prejudice its commercial interests. It noted that the withheld information:

"contains information regarding the capabilities of the product it provided to the Cabinet Office...[and]...shows information about the application interface, customisable elements of the product and a range of technical features. Such information is not publicly available and is only available to customers."
10. Having viewed a copy of the withheld information, the Commissioner is satisfied that Dataminr's description is accurate. The withheld information does indeed include descriptions of the software's user

interface and functionality – as well as screenshots that would show various features of the software.

11. The Commissioner recognises that the software is Dataminr's intellectual property and that its architecture and functionality are an integral part of the value of the software as a whole.
12. Disclosing the document would reveal information about the software's functionality which is not in the public domain and which could potentially be copied by competitors, to the detriment of Dataminr.
13. The Commissioner is therefore persuaded that disclosure would be likely to prejudice Dataminr's commercial interests and so section 43 of FOIA is engaged.

Public interest test

14. The Commissioner recognises that there is a public interest in understanding how Dataminr's software works and, more pertinently, how an organisation at the very heart of government is using that software.
15. The complainant has argued that software of this type has been used elsewhere to target activists. He provided several links to news articles which alleged that journalists and other peaceful activists had had their published activities on social media monitored.
16. More recently (and after the request was responded to), several newspapers have reported allegations, made by an anonymous whistleblower, that the UK government may have been monitoring the published social media posts of prominent opponents of the Covid-19 lockdown (the government has denied that individuals were targeted or that it took any action that could "impact anyone's ability to discuss and debate issues freely").¹
17. The Commissioner accepts the broader point that, given the advertised capabilities of the software, the potential for misuse exists if no adequate safeguards are in place.

¹ <https://www.dailymail.co.uk/news/article-11687675/Army-spied-lockdown-critics-Sceptics-including-Peter-Hitchens-suspected-watched.html>,
<https://pressgazette.co.uk/news/government-monitoring-of-covid-19-policy-media-critics-revealed/>

18. However, in the circumstances of this case, the Commissioner considers that the public interest should favour maintaining the exemption.
19. In the Commissioner's view, the strongest public interest lies in understanding how this product is being used, not in the precise mechanics of its operation. The information being withheld says nothing about what the software is actually doing for the public authority, any events or people it might have tracked, or the safeguards in place to prevent misuse.
20. There is information in the public domain which gives a reasonable overview of Dataminr's capabilities. For example, a blog on the company's website states that:

"From our early years, when public Twitter data was our first data source, until today, when it is one of thousands, public Twitter data has been a source that is full of unique and multi-dimensional value for detecting real-time events.

"Dataminr processes every public tweet in real-time. When a public tweet is published, Dataminr's AI platform receives that tweet instantaneously as a real-time input. Along with the text of the public tweet, Dataminr ingests a variety of public data fields attached to each tweet, totaling [sic] billions of real-time signals a day. Stated another way, Dataminr's platform processes tens of thousands of signals every second generated from Twitter alone.

"Dataminr runs its first AI models on each of these billions of daily inputs in 7.8 milliseconds. We use a broad and diverse spectrum of AI models to score, rank, filter, and cluster tweets, and identify, classify, and summarize events described within tweets. These AI models span supervised, semi-supervised and unsupervised learning. They extensively use neural networks, ranging from convolutional neural networks to recurrent neural networks, including long short-term memory networks. Our AI algorithms applied to tweets integrate a range of AI methods from several scientific fields, including natural language understanding, computer vision, and natural language generation."²

21. Having viewed the withheld information, the Commissioner is of the opinion that what it reveals the product's broad capability (as opposed to how to use its specific functionality, interface etc) does not go far

² <https://www.dataminr.com/blog/the-multi-dimensional-value-of-public-twitter-data-for-real-time-event-detection>

beyond what can already be deduced from the extract above or from other publicity material on Dataminr's website. Therefore disclosure would not add significantly to public understanding.

22. The Commissioner is therefore of the view that the balance of the public interest favours maintaining the exemption and allowing Dataminr to protect its intellectual property.

Part 2 – national security and security bodies

23. Section 23 of FOIA allows a public authority to withhold any information that was either supplied by or relates to a security body. The list of security bodies is contained within the exemption.
24. Section 24 of FOIA applies where withholding the information in question is required for the purposes of safeguarding national security.
25. 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. National security matters may cover:
- the security of the United Kingdom and its people;
 - the protection of democracy; the legal and constitutional systems of the state; as well as military defence;
 - action against a foreign state, if it indirectly affects the security of the UK ; and
 - reciprocal co-operation between the UK and other states in combating international terrorism.
26. It is not necessary to show that disclosing the information would lead to a direct or immediate threat to the UK. In a time of global terrorism, national security can depend on cooperating with others. This can involve protecting allies, cooperating with other countries in the fight against terrorism, as well as building relations with other prospective allies. This means that the exemption can be engaged to prevent a disclosure that would have adverse consequences for one of these partners, even if disclosure would not result in a direct or immediate risk of attack on the UK or its citizens.
27. Section 24 can only be engaged in respect of information that is not covered by section 23.
28. The public authority provided a list of the topics that the software had been used to monitor. It explained that disclosing the list would reveal what risks the UK Government was particularly concerned about during

the period in question. It would also, by omission, reveal the topics that weren't the subject of active monitoring.

29. The public authority provided the Commissioner with some examples of how the inclusion (or non-inclusion) in the list of particular topics would suggest particular vulnerabilities. The Commissioner is unable to provide any more detail without undermining the exemptions that have been applied, but he is satisfied that they demonstrate the causal link between disclosure and the detriment to national security.
30. The Commissioner also recognises that, were this information to be disclosed routinely, it would enable hostile actors to learn valuable information about when particular topics are added to, or removed from, the list of topics being monitored. That in itself would be valuable information as it would provide insight into how the public authority assesses various threats or vulnerabilities.
31. The Commissioner recognises that there is a relatively strong public interest in disclosure of this list as, unlike with the material sought in part 1 of the request, it would reveal information about how Dataminr's software is actually being put to use. The arguments set out above at paras 14-17 are equally relevant here.
32. However, the Commissioner also considers that there is an even stronger public interest in preventing the release of information that could damage national security.
33. Whilst some of the topics listed would be unsurprising (some topics overlap with topics referred to in the 2020 edition of the National Risk Register), others may be less so. The value of the list as a piece of work is its overview of what the public authority believes it needs to monitor and it is that overview that, if disclosed, would be harmful to the UK's national security.
34. Furthermore, for reasons that will be explained, not all the topics on the list fall under this exemption therefore, even if any threat to national security were overridden, disclosure would present only a partial view.
35. The Commissioner is therefore satisfied that the balance of the public interest favours maintaining section 24 of FOIA.
36. The public authority also argued that some of the topics on the list were exempt under section 23 of FOIA. It explained to the Commissioner that developments relating to certain topics would be disseminated to one or more security bodies and therefore these entries would reflect the priorities of the security body(ies) in question.

37. In this instance, the Commissioner has accepted at face value, the assertion, on behalf of the public authority, that the information relates to the work of one or more security bodies. This is for two reasons.
38. Firstly some of the topics on the list would self-evidently be of interest to security bodies – therefore there is a high likelihood, given the public authority's central role in matters of national security, that the topics do indeed reflect the priorities of security bodies.
39. Secondly, for the reasons set out above, the Commissioner is satisfied that section 24 of FOIA applies to the remainder of the topics that make up the list. Therefore, if any topics were not in fact covered by section 23, they would be exempt from disclosure under section 24.
40. The public authority has indicated to the Commissioner which topics it considers to be covered by which exemption. The Commissioner is satisfied that the topics the public authority has indicated as being covered by section 23 are covered by that exemption. The remaining topics are exempt under section 24.

Procedural matters

41. Section 17 of FOIA allows a public authority to delay the issuing of its refusal notice where it considers that a qualified exemption (ie. one that requires consideration of the public interest) applies and where it needs additional time to consider the balance of the public interest. There is no time limit on this delay and a public authority can delay issuing until "such time as is reasonable in the circumstances."
42. In the Commissioner's view, public authorities should take no more than an additional 20 working days to complete their public interest considerations.
43. The public authority has not indicated what circumstances prevented it from responding sooner and the Commissioner does not consider that such a delay was reasonable given the narrow extent of the information falling within scope and the fact that the public authority was also seeking to apply absolute exemptions (ie. exemptions that did not require a public interest test) to the same information.
44. As the public authority took an unreasonable amount of time to issue its refusal notice it breached section 17 of FOIA.

Right of appeal

45. 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

46. 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.
47. 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

Roger Cawthorne
Senior Case Officer
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF