Freedom of Information Act 2000 (FOIA)

Decision notice

Date:	**9 January 2023**
Public Authority:	**Chief Constable of West Yorkshire Police**
Address:	**Police HQ** **Laburnum Road** **Wakefield** **WF1 3QP**

Decision (including any steps ordered)

1. The complainant has requested information about a social media monitoring contract. The above public authority ("the public authority") refused to confirm or deny that it held relevant information, relying on sections 23 (security bodies), 24 (national security), 30 (criminal investigations) and 31 (law enforcement) of FOIA in order to do so.

2. The Commissioner's decision is that the public authority is entitled to rely on section 23(5) of FOIA to refuse to confirm or deny whether it holds information within the scope of element [4] of the request. The public authority has correctly engaged section 31(3) to neither confirm nor deny holding information within the scope of the remaining elements of the request and the balance of the public interest favours maintaining this exemption.

3. The Commissioner does not require further steps.

Request and response

4. On 5 April 2022, the complainant wrote to the public authority and requested information in the following terms:

> "I'm writing to you under the Freedom of Informtion [sic] Act (2000) to ask that you please disclose to me
>
> "[1] which social media platforms are monitored through your contract with Capita Business Services.

"[2] I'd also like to know what sorts of information the tool monitors, including whether or not it monitors protests, activists groups, or people critical of the police, as well as criminal activity - and which groups if relevent [sic] it monitors.

"[3] I'd also like the police to confirm or deny for me that the tool does or does not monitor the accounts of specific individuals, and how these are judged. For example, does this include politicans [sic], journalists, or "influencers".

"[4] Is this information shared with other security agencies, specifically those within the remit of the Ministry of Defence, and is there a data sharing agreement for this. Also, has a DPIA for this been completed?

"[5] I'd like a copy of the service agreements, not contract, shared between the company and police as part of this request."

5. The public authority responded on 6 May 2022. It refused to confirm or deny that it held information. It relied on sections 23(5), 24(2), 30(3) and 31(3) of FOIA in order to do so – a position it upheld at internal review.

6. During the Commissioner's investigation, the public authority clarified that it was only seeking to rely on section 23(5) in relation to element [4]. It no longer relied on section 30(3) to refuse to confirm or deny.

Reasons for decision

Element [4]

7. Section 23(5) of FOIA allows a public authority to refuse to confirm or deny holding information if doing so would in turn reveal something relating to one or more security bodies. Those bodies are defined in section 23(3) of FOIA and include the UK special forces.

8. Element [4] of the request seeks to understand whether data is or is not shared, by the public authority, with:

> "other security agencies, **specifically those within the remit of the Ministry of Defence**." [emphasis added]

9. The Commissioner considers that this reference would include any data the public authority shared (if indeed it had any to share) with the UK special forces – as they come within the remit of the MoD and might broadly be considered "security agencies."

10. As issuing a confirmation or a denial would indicate that data (if indeed such data existed) was or was not being brought to the attention of a security body, the public authority is therefore entitled to rely on section 23(5) of FOIA to refuse to confirm or deny whether it holds any information within the scope of this part of the request.

Elements [1], [2], [3] and [5]

11. Section 31(3) of FOIA allows a public authority to neither confirm nor deny whether it holds particular information if the mere act of confirming or denying that the information was held would, in itself, prejudice the ability of law enforcement bodies to carry out their functions effectively.

12. The public authority self-evidently has the function of preventing and detecting crime.

13. The Commissioner has accepted, in previous decision notices, that bodies charged with enforcing the law need to maintain a degree of ambiguity about their activities in order to enforce the law effectively. Disclosing information about the precise tactics such a body does or does not use would provide useful information to would-be criminals about the likelihood of their crimes being detected. This would potentially encourage certain crimes with a low risk of detection or would enable would-be criminals to counter the tactics being deployed by the public authority.

14. The Commissioner is therefore satisfied that section 31 is engaged in respect of element [1], as providing a confirmation or a denial that such a contract was held would reveal key information about the public authority's crime detection capabilities and therefore prejudice the prevention and detection of crime.

15. As elements [2], [3] and [5] are predicated on the assumption that the public authority holds information within the scope of element [1], the Commissioner accepts that the public authority cannot issue a confirmation or a denial that it holds information within the scope of these elements either. Not only would issuing a confirmation or a denial that information was held undermine its response to element [1], but these elements seek even more granular information about the public authority's crime detection capabilities.

Public interest test

16. The complainant argued that the public interest should strongly favour the issuing of a confirmation or a denial that the information was held.

17. He argued that there was the potential for such technology to be used to target "protest groups, journalists, politicians, and peaceful members of the public without consent" and therefore there was a strong public interest in "at least knowing the basics of how this software is used by law enforcement."

18. The public authority pointed to the strong public interest in allowing it to enforce the law effectively – without this ability being undermined by revealing some of its precise tactics.

19. The Commissioner considers that the public interest arguments in this case are finely balanced. On the one hand, he recognises that there is a strong public interest in ensuring that crime is being prevented effectively and that, when crimes are perpetrated, they are appropriately investigated. Revealing information that would assist criminals in avoiding detection is clearly not in the public interest.

20. However, on the other hand, the Commissioner (especially given his role as regulator of data protection legislation) considers that there is also a strong public interest in being transparent about where personal data is being collected and how it is being used. Whilst any information a person shares on social media is done voluntarily, individuals are not always aware of exactly how much information they are publishing and how that information might be used.

21. On balance, the Commissioner considers that the public interest favours neither confirming nor denying that this information is held. Firstly, the request only seeks a contract with a specific company, rather than whether **any** contract for such activities (with any firm) is in place – reducing the public value in the issuing of a confirmation or a denial.

22. Secondly, the Commissioner is aware from other complaints that the complainant has made similar requests to a number of police forces in the UK. If those forces do not respond to such requests in a consistent manner, it risks creating a "mosaic effect" whereby police capabilities across England are revealed – that in turn would be useful to criminals as it would reveal the areas of the country in which they would be most likely to escape detection.

23. The Commissioner is therefore satisfied that, in the circumstances of this case, the balance of the public interest favours maintaining the exemption.

Right of appeal

24. 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

25. 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.

26. 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