Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113 F. 01625 524510

Date: 17 July 2023

IC-239081-R6T5

Request

You asked us:

"I would like to request information about whether the Information Commissioner's Office monitors social media platforms for commentary about the Commissioner or the Office, sometimes called 'social media listening'.

1) Does the Commissioner's Office monitor social media platforms either in-house or outsourced to someone else? I am requesting recorded information but I am happy with a summary yes / no answer/

2) if yes, please provide recorded information about the purpose of this monitoring. This can be a summary or if there is a single information source that explains the purposes, that would be fine.

3) If yes, what is the purpose of the monitoring, how is the information used and who has access to it? If this is a limited number of people, I would like to know names and job titles, if it is a large group, please confirm whether the group includes the Information Commissioner and his deputies.

4) If yes and the service is outsourced, who is it outsourced to and what is the annual cost of the service?

5) If yes, please provide the most recent output from the monitoring that has been shared or circulated.

6) If yes, any recorded information about how the Commissioner complies with the UK GDPR with regard to personal data gathered via social media monitoring."

We received your request on 18 June 2023. We have handled your request under the Freedom of Information Act 2000 (the FOIA).

Our response

For ease of reading and reference, I have responded to each element of your request in a question/answer format.

You asked: *"Does the Commissioner's Office monitor social media platforms either in-house or outsourced to someone else? I am requesting recorded information but I am happy with a summary yes / no answer"*

In response, I can confirm that we do monitor our social media platforms (Twitter, LinkedIn, Facebook, and YouTube) via Hootsuite. We do this in-house. There are a handful of reasons that we do this, which I have detailed below in your other questions.

You asked: *"if yes, please provide recorded information about the purpose of this monitoring. This can be a summary or if there is a single information source that explains the purposes, that would be fine."*

I can confirm we hold information in scope of your request. There are three main reasons why we monitor social media. These are:

- To respond to direct engagement with us;
- To find news which is relevant to or likely relevant to our work; and
- For the purposes of FOI monitoring and enforcement.

I have detailed each of these separately.

Responding to direct engagement

Social media is a major way that people communicate. We monitor and reply to any questions, queries or information requests that are sent directly to us via social media.

We detail how we process personal data obtained via social media platforms in our privacy notice. Disclosure is exempt under s.21 as we've already made this available, but please see section headed "Social media" on this relevant page: How you can contact us | ICO. This page alludes to us treating engagement with our us through social media, where appropriate, as either an enquiry, a complaint, or an information request.

News relevant to or likely relevant to our work

We also monitor social media for any information that is relevant to what we do. For example, discussions about a data breach or if there are stories being reported in the news with a data protection or privacy element. To help us identify such information, we have 'saved searches' which is the held information. We check the following:

- Tweets to John Edwards Twitter account.
- Tweets that mention "the ICO".
- Tweets that include the ICO's site link.
- Tweets that mention "ICO registration letter" or "data protection fee".
- Tweets from the tech journalists list* that include the following phrases: "#journorequest", "journo request", "journo requests", "PR request", "#PRRequest", "DMs open", "get in touch", "data protection", "GDPR", "FOI", or "privacy".

* The tech journalists list is this publicly available list: https://twitter.com/i/lists/8096 (a Twitter account may be required to view the list).

Where information of interest is noted following these searches, then we may respond or pass information to a relevant person or department. The outcomes of these searches may also result in it being treated as an enquiry, complaint, or information request as detailed above.

FOI monitoring and enforcement

Finally, we look at Twitter as part of our FOI monitoring and enforcement work under the FOI and transparency regulatory manual. The reason we do this is because a stakeholder may tweet about a public authority whose FOI performance is alleged to be non-compliant and we can then act on that intelligence with the aim of improving the public authority's FOI performance. A practical example of this is in the Enforcement Notice we served again the London Borough of Lewisham where we saw critical comments on social media.

The relevant excerpt from the FOI and transparency regulatory manual on pages 8 and 9: *"Other evidence… The ICO sees a small percentage of the information requests made to public authorities via casework. We need to find ways to factor in how public authorities deal with the cases that don't get raised with us. We consider overall performance statistics from central government and will explore what other information is available in relation to other public authorities and*

sectors (such as data in Annual Reports, responses to previous requests that are available online etc) to make decisions on whether regulatory action is appropriate."

We also hold some recorded information about the purposes of the monitoring in minutes from the FOI monitoring and enforcement group dated 28 September 2022. The relevant excerpt is: *"Warren suggested reviewing social media feeds to identify PAs of concern– he mentioned CFOI, Martin Rosenbaum, Greenwood, FOI Man as possible twitter accounts to look at and to check the comments – probably some red herrings but worth doing every few days."*

You asked: *"If yes, what is the purpose of the monitoring, how is the information used and who has access to it? If this is a limited number of people, I would like to know names and job titles, if it is a large group, please confirm whether the group includes the Information Commissioner and his deputies."*

The purposing of the monitoring and how it is used is as detailed above. With regards to access, our monitoring is mediated through Hootsuite. I can confirm we hold information in scope of your request in that we hold a list of people authorised to access Hootsuite.

The platform is accessible by a member of our Public Advice and Data Protection Complaints Service as well as several members of our communications teams.

However, I consider that more detailed information (specific names, job titles) is exempt from disclosure under s.31 FOIA. I have provided full details below. However, in summary, providing a specific list of people with access would represent a cyber security risk.

I can confirm the Commissioner and his deputies do not have access to the ICO's Hootsuite platform, nor do they have direct access to any of the ICO's social media channels.

You asked: *"If yes and the service is outsourced, who is it outsourced to and what is the annual cost of the service?"*

The service is not outsourced and therefore no information is held.

You asked: *"If yes, please provide the most recent output from the monitoring that has been shared or circulated."*

Our monitoring covers treating contact with us as an enquiry, a complaint, or an information request as well as specifically checking for information in certain places and sometimes using particular keywords (as detailed above). I consider it is very unlikely that your request for the 'most recent output' is a request for the latest enquiry, complaint, or information request we have created as a result of contact via social media.

I have therefore interpreted it as a request for any output concerning our monitoring where the output is some kind product designed and intended to be circulated.

With that in mind, I can confirm we do hold information in scope in relation to the 'saved searches' we've detailed above. The following is an excerpt from an email shared with our wider communications team, our Relationship Management Service, and our Parliamentary and Government Affairs team on 13 June 2023:

"An interesting Twitter thread I've noticed on the story of the woman jailed for taking abortion pills after the time limit.

Sophia Smith Galer (Senior Reporter at VICE focussing on investigations across sexual and reproductive health rights) highlighted a privacy issue in this story. The defendant in the case said "she said she didn't know how long she'd been pregnant. But police gathered web searches and messages which disputed this." She then has gone on to discuss the "digital information" that has been asked for via police warrants in relation to abortion crimes in the USA.

Thread here: https://twitter.com/sophiasgaler/status/1668260538940268545?t=Y41J4Jg7Gz8Gs_kEpE7Fbw&s=09".

However, we do not hold any information concerning the outputs of our monitoring and enforcement work. This is because the FOI monitoring and enforcement group deletes monitoring information within 5 days of any meeting and the last report would have been produced in May 2023.

You asked: *"If yes, any recorded information about how the Commissioner complies with the UK GDPR with regard to personal data gathered via social media monitoring."*

We do hold information in scope of this part of your request. The section of our privacy notice details how we process personal data gathered through contacting us on social media is here: How you can contact us | ICO (see "Social media").

However, we do not hold a specific policy that covers social media monitoring exclusively.

This concludes our response to your request. I hope you find the above information useful.

Exemption applied: FOIA s.31

Some of the information you have requested is exempt from disclosure under section 31(1)(a) of the FOIA. We can rely on this section where disclosure:

"would, or would be likely to, prejudice… the prevention or detection of crime"

Section 31 is not an absolute exemption, and we must consider the prejudice or harm which may be caused by disclosure. We also have to carry out a public interest test to weigh up the factors in favour of disclosure and those against.

I have taken cyber security advice about the risks associated with releasing information about specific people who have access to a publicly accessible system (in this case, Hootsuite). The advice I received was that malicious actors are constantly looking for information about organisations in order to facilitate attacks. Disclosing information about people who have access to systems has been described to me as a 'gift' to such malicious actors, who at the very least could use those credentials to brute force access or engage in phishing attacks.

I consider that by making such information readily and easily available, it would make it much easier for such malicious actors to enact cyber attacks. Or, to put it in terms of prejudice to the ICO, it would prejudice our ability to prevent cyber attacks on us and the systems we use because we would be handing confirmation of part of the credentials used to access such systems which could be used to launch attacks.

With this in mind, we have then considered the public interest test for and against disclosure.

In this case the public interest factors in disclosing the information are:

- Improving transparency in how the ICO monitors and engages with social media, as well as who is behind such activities.

The factors in withholding the information are:

- There is very little public interest value in knowing *specifically* who has access to social media channels, taking into account associated risks.
- There is a public interest in the ICO allocating resources most effectively, and more resources would need to be allocated to cyber security if we weren't employing good cyber security practices, such as by disclosing partial access credentials of a system.
- It would make it harder for the ICO to regulate other organisations on best practice when the ICO is itself making disclosures that create risks with little to no benefit and against best practice advice.

Having considered these factors, we are satisfied that it is appropriate to withhold the information.

Next steps

You can ask us to review our response. Please let us know in writing if you want us to carry out a review. Please do so within 40 working days.

You can read a copy of our full review procedure here.

If we perform a review but you are still dissatisfied, you can complain to the ICO as regulator of the FOIA. This complaint will be handled just like a complaint made to the ICO about any other public authority.

You can raise a complaint through our website.

Your information

Our Privacy notice explains what we do with the personal data you provide to us, and set out your rights. Our retention schedule can be found here.

Yours sincerely

Information Access Team
Risk and Governance Department, Corporate Strategy and Planning Service
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
ico.org.uk twitter.com/iconews