

Freedom of Information Act 2000 (FOIA)

Decision notice

Date: 23 November 2022

Public Authority: Commissioner of Police of the Metropolis
Address: New Scotland Yard
Broadway
London
SW1H 0BG

Decision (including any steps ordered)

1. The complainant made a request to the Metropolitan Police Service (the "MPS"), for information held in its Counter Terrorism Internet Referral Unit (CTIRU) dedicated database. The MPS refused to provide the requested information, relying on sections 24(1) (National security), 30(1)(a) (Investigations and proceedings) and 31(1)(a) (Law enforcement) of FOIA. It also refused to confirm or deny holding any further information by virtue of section 23(5) (Information supplied by, or relating to, bodies dealing with security matters) of FOIA.
2. The Commissioner's decision is that section 31 of FOIA is properly engaged and the public interest favours maintaining the exemption. He also finds that the MPS was entitled to rely on section 23(5) of FOIA. No steps are required.

Background

3. This is a follow up request to one which the Commissioner has previously considered and found to be exempt by virtue of section 14 (Vexatious requests). The earlier decision can be found online¹.
4. The Commissioner has previously viewed the training version of the CTIRU database so is familiar with its content and structure.
5. The MPS has explained:

“The CTIRU was set-up following a review from the 2005 London terrorist attacks, whereby it was clear that, at that time, terrorist groups could freely use the internet to post their material unchallenged. The CTIRU investigates terrorist use of the internet. It views online content and seeks to prevent terrorist use of the internet”.

Request and response

6. On 5 November 2021, the complainant wrote to the MPS and requested information in the following terms:

“I would like to request information from the Counter Terrorism Internet Referral Unit (CTIRU) database.

I would like to request a list of all entries from the start of 2020 until present day.

For each list entry I would like to receive the information listed under:

 - Date/Time
 - Content Title”.
7. On 16 November 2021, the MPS responded. It refused to provide the requested information, relying on sections 24(1), 30(1)(a) and 31(1)(a) of FOIA. It also refused to confirm or deny holding any further information by virtue of section 23(5).

¹ <https://ico.org.uk/media/action-weve-taken/decision-notices/2021/4019030/ic-74027-g7v2.pdf>

8. The complainant requested an internal review on 27 November 2021.
9. The MPS provided an internal review on 23 December 2021, in which it maintained its original position.

Reasons for decision

Section 23 - Information supplied by, or relating to, bodies dealing with security matters

10. The MPS explained to the complainant:

“In relation to any additional information which may or may not be held which is relevant to your request, the MPS has relied on Section 23(5) of the Act – Information supplied by, or relating to, bodies dealing with security matters”.

11. Section 23(5) provides an exemption from the duty imposed by section 1(1)(a) to confirm or deny whether information is held if to do so would involve the disclosure of information, whether or not recorded, that relates to, or was supplied by, any of the security bodies listed in section 23(3). This is a class-based exemption, which means that if the confirmation or denial would have the result described in section 23(5), this exemption is engaged. It is not subject to the public interest test.
12. In line with the Tribunal case **EA/2010/0008**, the approach of the Commissioner is that the balance of probabilities is the correct test to apply. This means that for section 23(5) to be engaged, the evidence must suggest to a sufficient degree of likelihood (rather than certainty) that any information held that falls within the scope of the request would relate to, or have been supplied by, a body specified in section 23(3).
13. In this case, the Commissioner considers it clear that the subject matter of the request – counter terrorism – is within the area of the work of bodies specified in section 23(3). He also accepts that it is likely that, if any further information as described in the request did exist, this would be likely to relate to work involving security bodies.
14. The Commissioner accepts that, on the balance of probabilities, any such information falling within the scope of the complainant’s request would relate to, or have been supplied by, a body or bodies listed in section 23(3). His conclusion is therefore that section 23(5) is engaged.

Section 31 – Law enforcement

15. Section 31 of FOIA creates an exemption from the right to know if disclosing the information would, or would be likely to, prejudice one or more of a range of law enforcement activities.
16. In this case, the MPS is relying on sections 31(1)(a) of FOIA in relation to all the withheld information. This subsection states that information is exempt if its disclosure would, or would be likely to, prejudice the prevention or detection of crime.
17. In order to engage a prejudice based exemption such as section 31 there must be likelihood that disclosure would, or would be likely to, cause prejudice to the interests that the exemption protects. In the Commissioner's view, three criteria must be met in order to engage a prejudice based exemption:
 - Firstly, the actual harm which the public authority alleges would, or would be likely to, occur if the withheld information was disclosed has to relate to the applicable interests within the relevant exemption;
 - Secondly, the public authority must be able to demonstrate that some causal relationship exists between the potential disclosure of the information being withheld and the prejudice which the exemption is designed to protect. Furthermore, the resultant prejudice which is alleged must be real, actual or of substance; and,
 - Thirdly, it is necessary to establish whether the level of likelihood of prejudice being relied upon by the public authority is met – ie disclosure 'would be likely' to result in prejudice or disclosure 'would' result in prejudice.
18. Consideration of the exemption at section 31 is a two-stage process: even if the exemption is engaged, the information should be disclosed unless the public interest in maintaining the exemption outweighs the public interest in disclosure.

The applicable interests

19. The first step in considering whether this exemption is engaged is to address whether the prejudice predicted by the public authority is relevant to the law enforcement activities mentioned in section 31(1)(a) - the prevention or detection or crime. With respect to law enforcement

activities, the Commissioner recognises in his published guidance² that section 31(1)(a) will cover all aspects of the prevention and detection of crime.

20. The MPS has explained that:

"... the requested information would include detail that identifies, or can be linked to, police investigations - including those that are still ongoing. The disclosure of such information would be of value to those seeking to distribute extremist material online by identifying the type of content that is, or is not, recorded on the CTIRU database".

And:

"... disclosure of the requested information would cause operational harm to the MPS, and its national counterparts, and affect our ability to fulfil the core function of law enforcement effectively in the future. Additionally, disclosure of the requested information would place the public at greater risk of terrorist activity, if the MPS disclosed the sensitive information contained on the CTIRU database".

21. The Commissioner acknowledges that the arguments presented by the MPS refer to prejudice to the prevention or detection of crime and to the apprehension or prosecution of offenders and that the appropriate applicable interests have therefore been considered.

The nature of the prejudice

22. The Commissioner next considered whether the MPS has demonstrated a causal relationship between the disclosure of the information at issue and the prejudice that section 31(1)(a) is designed to protect. In his view, disclosure must at least be capable of harming the interest in some way, ie have a damaging or detrimental effect on it.

23. The MPS has explained:

"It is important to note that the UK does face a serious and sustained threat from violent extremists and protestors and this threat is greater in scale and ambition than any of the terrorist threats in the past. Government reports suggest that at any one

² <https://ico.org.uk/media/for-organisations/documents/1207/law-enforcement-foi-section-31.pdf>

time the police and security agencies are contending with many terrorist plots, terrorist groups or networks and individuals who are judged to pose a threat to the well-being of the UK and/or UK interests.

In this current environment of an increased threat of terrorist activity, releasing this information may assist an extremist faction, or a protest group or any other group/individual whose intent it is to cause harm with the opportunity to undermine the safeguarding of national security.

Members of the public would be placed in greater danger if a disclosure facilitated access to extremist websites which allowed those involved in terrorist activity the opportunity to promote further their ideological beliefs".

24. The complainant has argued: "I don't see how this very limited information (date / time / title) would help people find terrorist information".

25. However, the MPS explained that:

"Your request for information may seem harmless on its own given [sic], however we have to be mindful [sic] of the effect of disclosure on policing tactics and procedures used to combat terrorism. Those with the necessary criminal intent, inclination and capacity could use the information to gain an operational advantage over the MPS as the information can be classed as operational 'intelligence' and operationally sensitive. Disclosure would compromise the police service function of the prevention and detection of crime".

And:

"The MPS has a statutory role in investigating criminal offences and deploys a range of tactics and investigative techniques to do so. Disclosure of the requested information would, in this case, provide the public with an in depth knowledge of policing tactics, intelligence and strategies. This would be harmful, as this would inform the offender of the capabilities available to the MPS in investigating terrorist offences and apprehending offenders.

Individuals (including criminals) 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, which may further encourage criminal activity by exposing potential vulnerabilities.

More broadly, disclosing details of intelligence held and investigative options available to the MPS, particularly if a series of requests are made and responded to, would inform and embolden the offender. An informed and emboldened offender would be more likely to commit offences and be successful in doing so. The public interest does not support disclosure of the requested information when doing so would compromise the Met's ability to detect and investigate crimes and/or would encourage or facilitate crime.

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 organised crime 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.

FOIA disclosures are placed into the public domain and disclosures which appear innocuous, pieced together with other disclosures can be used in a 'mosaic effect' to give a fuller picture to those wishing to evade detection and valuable intelligence to criminals".

26. The MPS has also explained:

"... disclosure of the requested information would cause operational harm to the MPS, and its national counterparts, and affect our ability to fulfil the core function of law enforcement effectively in the future. Additionally, disclosure of the requested information would place the public at greater risk of terrorist activity, if the MPS disclosed the sensitive information contained on the CTIRU database.

It is considered that disclosure would hinder the ability of the MPS to prevent and detect terrorist acts if sensitive information and intelligence is disclosed and the intelligence and capabilities available to the MPS at specific points in time made public. This information could be used by terrorists to try and evade detection and to assist with their plans for acts of terror".

27. The Commissioner has viewed a sample of the data in the 'title' field of the database, which is where he considers the main harm would lie, ie the date / time would be of limited value in isolation as this would reveal little content (unless someone was trying to ascertain whether a particular event may have been recorded on the database). He is satisfied that this data would reveal the types of intelligence held on the database and, coupled with the date / time as requested, could inform

criminals / terrorists with vital information about what is or isn't known about their activities.

Likelihood of prejudice

28. With regard to the likelihood of prejudice in this case, the MPS arguments are presented at the level of 'would' prejudice.

Is the exemption engaged?

29. In a case such as this, it is not enough for the information to relate to an interest protected by section 31(1)(a), its disclosure must also at least be likely to prejudice those interests. The onus is on the public authority to explain how that prejudice would arise and why it would occur.
30. The Commissioner recognises the importance of protecting information which, if disclosed, would undermine law enforcement activity or make someone more vulnerable to crime.
31. Having considered the arguments put forward by the MPS, the Commissioner accepts that disclosure would be likely to be useful to someone intent on establishing details about the type of information which the MPS holds in its CTIRU database, ie it is of particular use to those seeking to commit crimes and acts of terrorism. Consequently, the Commissioner is satisfied that its disclosure would be likely to represent a real and significant risk to law enforcement matters.
32. As the Commissioner accepts that the outcome of disclosure predicted by the MPS would occur, he is therefore satisfied that the exemption provided by section 31(1)(a) is engaged.

Public interest test

33. Section 31 is a qualified exemption. The Commissioner must now consider whether, in all the circumstances of the case, the public interest in maintaining the exemption at section 31(1)(a) of FOIA outweighs the public interest in disclosing the information requested by the complainant.

Public interest considerations favouring disclosure

34. The complainant did not provide any arguments.
35. The MPS argued:

"Access to information is essential to democratic discourse and open and informed debate. The disclosure of information facilitates

transparency and accountability and may increase citizens' empowerment and participation in society".

36. It also recognised the public interest in assuring the public that the MPS is appropriately and effectively engaging with the threat from criminals.

Public interest arguments in favour of maintaining the exemption

37. The MPS argued that there is a very strong public interest in safeguarding law enforcement methodology and capabilities.

38. It further explained:

"Disclosure of the requested information would compromise law enforcement, which would hinder the prevention and detection of terrorist and extremist crimes. It is considered that the threat of terrorism will increase as more crimes are committed as a result of terrorists gaining access to subversive material which incites or assists others to participate in these acts, therefore placing the general public at a greater risk and a fear of crime will be realised.

By revealing the requested information, some of those who disseminate extremist material will be able to determine that they are known to the MPS, which could lead to them setting up different websites to publicise their cause, therefore escaping the MPS radar. A release of information which alerts a potential terrorist that the MPS is aware of their activities, and therefore disrupts any investigation, will lead to the need for more police resources to reassure and protect the public".

Commissioner's conclusion

39. In carrying out the statutory balancing exercise in this case, the Commissioner considers that appropriate weight must be afforded to the public interest inherent in the exemption - that is, the public interest in avoiding likely prejudice to law enforcement matters. Clearly, it is not in the public interest to disclose information that may compromise the police's ability to accomplish its core function of law enforcement.
40. In that respect, he recognises that there is a very strong public interest in protecting the law enforcement capabilities of a police force and he considers that appropriate weight must be afforded to the public interest inherent in the exemption - that is, the public interest in avoiding prejudice to the prevention or detection of crime.
41. The Commissioner also recognises the need to ensure transparency and accountability on the part of the police. However, he finds that there is a stronger public interest in ensuring that precise details regarding the

content of the CTIRU database should not be revealed. Whilst the complainant does not consider the limited data requested to be sensitive, the Commissioner understands the MPS' concerns about the mosaic approach that those seeking to evade detection will take when trying to source any information to their advantage. Even knowing the date and time that something was logged on the database may give an indication as to whether or not the MPS is aware of an incident that has happened. This, coupled with a title describing details of that event, could be used to confirm this.

42. Policing techniques can only be properly effective when full policing capabilities are not publicly known; disclosure of the data requested would be to the detriment of the wider public, as those seeking to evade the law would be able to ascertain how best to do so.
43. In the circumstances of this case, the Commissioner considers that the public interest in maintaining the exemption readily outweighs the public interest in disclosing the information. It follows that the MPS was entitled to rely on section 31(1)(a) of FOIA to refuse to disclose the requested information.
44. In light of his findings, the Commissioner does not consider it necessary to consider the other exemptions cited. His initial view however, is that they are all likely to be properly engaged.

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

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