Freedom of Information Act 2000 (FOIA)

Decision notice

Date: **4 November 2021**

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

Decision (including any steps ordered)

1. The complainant made multiple requests to the Metropolitan Police Service (the "MPS"), for information held in its Counter Terrorism Internet Referral Unit (CTIRU) dedicated database. The MPS initially found the requested information to be exempt by virtue of sections 23(5) (Information supplied by, or relating to, bodies dealing with security matters), 24(1) (National security), 30(1)(a) (Investigations and proceedings), 31(1)(a) (Law enforcement) and 44(1)(a) (Prohibitions on disclosure) of the FOIA. During the Commissioner's investigation this was revised and the MPS found the requests to be vexatious under section 14(1) (Vexatious or repeated requests) of the FOIA.

2. The Commissioner's decision is that the MPS was entitled to find the requests to be vexatious. No steps are required.

Background

3. The requests refer to the CTIRU. There is little information publicly available about this unit and its work, however, the Commissioner has located the following statement:

> *"The core business of the CTIRU involves assessing and identifying online material, believed to be hosted in the UK, which is assessed to breach Terrorist Act (TACT) legislation.*

… The CTIRU, generally via public referrals, assesses content, which, on occasion falls short of terrorism but which breaches other legislation – for example sections of the 1986 Public Order Act (including those racially or religiously aggravated as defined by S1 of the 1998 Crime & Disorder Act)"[1].

4. The MPS has also confirmed to the Commissioner that:

"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. Where such material breaches UK law it often take a copy of the material and then contacts the hosting provider to make them aware that they are hosting it - often hosting companies are unaware of this".

5. The Commissioner has not viewed the database. She was invited to view it *in situ* as it was not technically possible for the MPS to provide her with extracts, but she did not consider this to be necessary in order to reach a decision in this case.

Request and response

6. Following earlier requests about the CTIRU, on 18 September 2020 the complainant wrote to the MPS and made the following three information requests (numbered for convenience):

"1) I would like to request information from the Counter Terrorism Internet Referral Unit (CTIRU) dedicated database used to log all investigations.

I would like to request a list of all entries from the start of 2018 until present day.

For each list entry I would like to recieve [sic] *the information listed under:*

-Date/Time

[1] https://committees.parliament.uk/writtenevidence/21720/html/

-URL
-Content Title".

"2) I would like to request a cope [sic] *of entities that are listed under "Evidential capture – file copy of material that is available for investigation/court case" and listed on the Counter Terrorism Internet Referral Unit (CTIRU) dedicated database used to log all investigations.*

I would like to request everything that were [sic] *stored between 1 January 2020 and 1 April 2020".*

"3) I would like to request digital files of the media content listed on the Counter Terrorism Internet Referral Unit (CTIRU) dedicated database used to log all investigations.

I would like to request all of the files that were stored between 1 January 2020 and 1 April 2020".

7. On 12 October 2020, the MPS acknowledged all three requests and advised that it needed more time in which to consider the public interest test.

8. On 13 October 2020, the MPS refused all three requests citing sections 23(5), 24(1), 30(1)(a) and 31(1)(a)of the FOIA.

9. The complainant requested an internal review on 3 November 2020.

10. The MPS provided an internal review on 1 December 2020, in which it added reliance on section 44(1)(a) of the FOIA.

11. During the Commissioner's investigation, the MPS revised its position, finding the requests to be vexatious under section 14(1) of the FOIA.

Scope of the case

12. The complainant contacted the Commissioner on 1 December 2020 to complain about the way his requests for information had been handled.

13. Further information was required from him, which was provided by 16 December 2020.

14. The Commissioner subsequently asked the complainant for his grounds of complaint which were also provided.

15. Following the MPS's revised position and citing of section 14(1), the Commissioner again requested the complainant's views. He responded

advising that he did not believe that compliance would be 'grossly oppressive' and that, as he was requesting simple information from a pre-existing database, he believed its retrieval should be very easy. He added:

> *"a) I do not think that any of this basic, generic information would be exempt – so the police would not have to spend hours going through records as it suggests.*
>
> *b) The information could be pulled directly from the database – I think it would be totally unnecessary to go back to "each record" and manually process it as the Met suggests".*

16. He also queried why the MPS had not cited the cost limit which is covered in the analysis below.

17. The Commissioner will consider whether or not the requests were vexatious, below.

Reasons for decision

Section 14 – Vexatious or repeated requests

18. Section 14(1) of the FOIA states that section 1(1) does not oblige a public authority to comply with a request for information if the request is vexatious. The section is not subject to a public interest test.

19. The term 'vexatious' is not defined in the FOIA. The Upper Tribunal considered the issue of vexatious requests in the case of the *Information Commissioner v Devon CC & Dransfield (Dransfield)*. The Tribunal commented that vexatious could be defined as the "*manifestly unjustified, inappropriate or improper use of a formal procedure*". The Tribunal's definition clearly establishes that the concepts of proportionality and justification are relevant to any consideration of whether a request is vexatious.

20. In the *Dransfield* case, the Upper Tribunal also found it instructive to assess the question of whether a request is truly vexatious by considering four broad issues:

(1) the burden imposed by the request (on the public authority and its staff),
(2) the motive of the requester,
(3) the value or serious purpose of the request and
(4) harassment or distress of and to staff.

21. The Upper Tribunal did, however, also caution that these considerations were not meant to be exhaustive. Rather, it stressed the:

> *"…importance of adopting a holistic and broad approach to the determination of whether a request is vexatious or not, emphasising the attributes of manifest unreasonableness, irresponsibility and, especially where there is a previous course of dealings, the lack of proportionality that typically characterise vexatious requests"* (paragraph 45).

22. The Commissioner has published guidance on dealing with vexatious requests[2]. That guidance includes a number of indicators that may apply in the case of a vexatious request. The fact that a request contains one or more of these indicators will not necessarily mean that it must be vexatious. All the circumstances of the case will need to be considered in reaching a judgement as to whether a request is vexatious.

23. As discussed in the Commissioner's guidance, the relevant consideration is whether the request itself is vexatious, rather than the individual submitting it. A public authority can also consider the context of the request and the history of its relationship with the requester when this is relevant. The Commissioner's guidance states:

> *"The context and history in which a request is made will often be a major factor in determining whether the request is vexatious, and the public authority will need to consider the wider circumstances surrounding the request before making a decision as to whether section 14(1) applies".*

24. Sometimes it will be obvious when a request is vexatious, but sometimes it may not. In that respect, the Commissioner's guidance states:

> *"In cases where the issue is not clear-cut, the key question to ask is whether the request is likely to cause a disproportionate or unjustified level of disruption, irritation or distress".*

25. In the Commissioner's view, section 14(1) is designed to protect public authorities by allowing them to refuse any requests which have the potential to cause a disproportionate or unjustified level of disruption, irritation or distress. This will usually involve weighing the evidence about the impact on the authority and balancing this against the

[2] https://ico.org.uk/media/for-organisations/documents/1198/dealing-with-vexatious-requests.pdf

purpose and value of the request. This should be judged as objectively as possible; in other words, would a reasonable person think that the purpose and value are enough to justify the impact on the public authority.

26. In particular, the Commissioner accepts that there may be cases where a request could be considered to be vexatious because the amount of time required to review and prepare the information for disclosure would place a grossly oppressive burden on the public authority. This is the position adopted by the MPS in this case.

27. The Commissioner believes that there is a high threshold for refusing a request on such grounds. This means that a public authority is most likely to have a viable case where:

- the requester has asked for a substantial volume of information and
- the authority has real concerns about potentially exempt information, which it will be able to substantiate if asked to do so by the Commissioner and
- any potentially exempt information cannot easily be isolated because it is scattered throughout the requested material.

28. It is the MPS's position that to comply with the requests would be burdensome to the MPS and would require a disproportionate effort which cannot be justified by the purpose and value of the requests.

The complainant's views

29. The complainant's views regarding the citing of section 14 are outlined above. He believes that the impact of his request would be minor and that it is fully justified. He does not consider that compliance would cause a disproportionate or unjustified level of disruption or distress and considers that it is clearly not a request that is intentionally annoying or disruptive. In his view: *"… it seems extremely reasonable to request information from this database and it should be very simple to provide it"*.

The MPS's views

30. The MPS has claimed that to comply with the requests would impose a grossly oppressive burden which is not covered by the section 12 appropriate cost limit. This is because a public authority cannot claim section 12 for the cost and effort associated with considering exemptions or for redacting exempt information.

31. It went on to consider the points which the Commissioner has referred to above, and advised the complainant as follows:

*"**1 - The requester has asked for a substantial volume of information***

*You have requested a list of **all entries** from the start of 2018 until present day and to include -Date/Time, -URL, -Content Title. The nature of this request is considered wide in scope for all entries for a period over 3 years and is also considered a substantial volume of information.*

In [an earlier request made by the complainant] *… You were provided with the volume of CTIRU requests to remove content deemed in breach of UK terrorism laws from 2017 to 2019, as follows*

Year	***** Flagged***	***URLs Removed***
2017	*41,588*	*34,250*
2018	*8,433*	*7,452*
2019	*5,503*	*3,431*

*** Flagged = takedown request*

You were also advised 'It should be noted that removed figures can be higher than referred due to platforms taking time to remove content (i.e. if content is referred to a platform towards the end of a month/year, it is possible that this content would not be removed until the next month or months after). In addition, the CTIRU are not always contacted by the platform to confirm that they have removed the content. Therefore the removal figure relies on checking that the content has been removed ...'

It can be seen that this is a substantial volume of information to prepare. This would not include the time taken to prepare the remaining requests for the evidential capture and digital files of the media content listed on the CTIRU database for a 3 month period 1/1/2020 to 1/4/2020.

2 - The authority has real concerns about potentially exempt information, which it will be able to substantiate if asked to do so by the ICO

Within [an earlier request made by the complainant], *concerning the **list of platforms** you were advised:*

'…Please also note that it is not possible to make public a list of the platforms to which referrals have been made. ***This information could be used to identify or highlight where terrorist propaganda might be best uploaded.*** *This information would be considered exempt by the MPS.'*

All of the requested information will have to be considered. The work which is required to be undertaken by a member of police staff is substantial and includes reading through potentially thousands of records to determine if it contains exempted material. The harm has previously been highlighted in response to [an earlier request made by the complainant]*, as follows:*

'… the CTIRU was the first unit in the world set up to tackle the proliferation of illegal terrorist and violent extremist content on the internet. It works with service providers to instigate the removal of access to terrorist and extremist material, which breaks their terms of service. Once such material has been identified, the CTIRU sends the internet service provider an advisory note, seeking the removal of the material. Publication of such material can also lead to those who publish it being investigated for offences under the Terrorist Act 2006.'

'Police forces work in conjunction with other agencies and on a daily basis information is freely shared in line with information sharing protocols. Modern day policing is intelligence led and this is particularly pertinent with regard to both law enforcement Official Sensitive Official Sensitive and national security. The public expect police forces to use all powers and tactics available to them to prevent and detect crime or disorder and maintain public safety…

In order to counter criminal and terrorist behaviour it is vital that the police have the ability to work together, to obtain intelligence within current legislative frameworks to assist in the investigative process to ensure the successful arrest and prosecution of offenders who commit or plan to commit acts of terrorism.

To achieve this goal, it is vitally important that information sharing takes place between police officers, members of the public, police forces as well as other security law enforcement bodies within the United Kingdom and internationally if appropriate. This information sharing supports counter-terrorism measures in the fight to deprive terrorist networks of the ability to commit crime.
…

When considering the public interest it is highlighted that the Police Service relies heavily on the public and other law enforcement

agencies to provide information to assist in criminal investigations. As stated within above the public has an expectation that any information they provide to be treated in confidence and in line with the APP Information Management Module. Anything which places that confidence at risk, no matter how generic, would undermine any trust or confidence other agencies and individuals have in the Police Service.

The effective delivery of operational law enforcement takes priority and is at the foremost of the MPS to ensure the prevention and detection of crime is carried out and the effective apprehension or prosecution of offenders is maintained with the ultimate aim of ensuring National Security is not compromised.'

In response to [an earlier request made by the complainant]*, the MPS also advised you:*

'To disclose the requested list of websites would identify where terrorist material might be held which would allow those intent on causing harm or at risk of being radicalised with information that would allow them to view extremist media content. ***As this material is illegal to possess or view by a member of the public without lawful excuse, it may well form evidence in criminal proceedings or be subject to an ongoing investigation****. This would compromise our law enforcement functions, have a negative effect on national security and may impact on any current investigation. As such Sections 24(1), 30(1)(a) and 31(1)(a) of the Act are engaged.*
…

The evidence of overall harm also highlighted the prejudice resulting from disclosure as follows:

'…disclosure of these websites, could provide potential terrorists / extremists with access to material which encourages / glorifies acts of terrorism or which otherwise incites or assists others to participate in such acts, this would compromise the MPS's ability to accomplish its core function of law enforcement.

The threat from terrorism cannot be ignored. It should be recognised that the international security landscape is increasingly complex and unpredictable. The UK faces a sustained threat from violent terrorists and extremists ... With the current threat level to the UK given as 'severe, the Home Office website explains that 'this means that a terrorist attack is likely'.
http://www.homeoffice.gov.uk/counter-terrorism/current-threat-level/

In consideration of the ramifications of this threat level, it would not be wise to disclose any information, which would enable those with a criminal intent to gain an operational advantage of over the MPS, hindering our ability to detect and prevent crime and affect the safety of the public at a national level.

Members of the public would be placed in greater danger if extremist websites were disclosed which allowed those involved in terrorist activity the opportunity to promote further their ideological beliefs.'

Under factors favouring non-disclosure, I refer to the following comment:

'By revealing the requested information could allow those who create such websites to be aware 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.'

Finally, the following Balance test is also relevant here:

'The security of the country is of paramount importance and the MPS will not divulge any information, which would undermine National Security or compromise law enforcement or place individuals at risk. Whilst there is a public interest in the transparency of policing, and in this case providing assurance that the police service is appropriately and effectively engaging with the threat posed by terrorist activity, there is a very strong public interest in safeguarding both national security and the integrity of police investigations and operations in the highly sensitive subject of terrorism and extremism.

As much as there is a public interest in knowing that policing activity is appropriate and balanced in matters of national security this will only be overridden in exceptional circumstances. Any disclosure of information held by that would demonstrate online terrorism and extremism websites of interest to the MPS are sensitive issues of intelligence value to a terrorist.

The MPS will not divulge information if it is likely that it will compromise the work of the Police Service or place members of the public at risk. It is known that terrorist cells will try to radicalise

people and children online, so that they believe in their ideology, in order to encourage them to commit acts of terror.

It is also considered in these circumstances that there is a public interest in safeguarding the integrity of any police investigations and operations that may be ongoing. There is a need to ensure that any investigation is not compromised by releasing information before the conclusion of a case.'

In the subsequent Internal Review [to an earlier request made by the complainant]*, the MPS additionally considered that the publication of such details, such as Date/Time -URL, -Content Title and file copy of material that is available for investigation/court case and digital files of the media content as would be held within the CTIRU database, were prohibited from being released (s.44(1)(a) FOI) by virtue of any other enactment, namely section 2 of the* ***Terrorism Act 2006***.

3 - Any potentially exempt information cannot easily be isolated because it is scattered throughout the requested material.

Having now considered the requested information, I am satisfied that exempted information cannot be isolated because it is scattered throughout the request.

To provide you with a reasonable estimation if it took between 3 - 4 minutes to read through each record to review and prepare a response would equate to between 50 and over 66 hours for every 1000 records, for this aspect of work to be undertaken".

32. The MPS concluded that the amount of time required to review and prepare the information for disclosure would impose a grossly oppressive burden. Furthermore, were such work undertaken, then it is likely that much of the content requested would be exempt from disclosure based on the rationale provided above.

33. The MPS also explained to the Commissioner that CTIRU officers record their investigations in the database. This will include various basic typed fields, however, material is often in the form of a video, audio file, still image or displayed writing (PDF). Such media items are either captured in full (copy of the video) or a screenshot is taken.

34. Most cases are complex and the material could be required for a court case in the future.

35. CTIRU case officers video record their computer screen whilst viewing the material. These videos are known as "evidential captures". These

video files are saved and displayed on a container field on the database investigation record. As they are video files they can often be large files.

36. The database, whilst effective for business needs, has limited functionality to enable quick and easy access to media files. Efforts are ongoing to design and build a new database for the CTIRU.

37. The database has two areas – the investigation database (DB1) and a separate URL database (DB2) for logging the URLs found in the investigation. It is not known how many videos files are stored on these as there is no method to do a count of these files other than going through all the records individually.

The Commissioner's view

38. The Commissioner would initially like to comment on part of the revised submission which the MPS sent to the complainant after finding the request to be vexatious, albeit the complainant did not refer to it in his subsequent grounds of complaint. The MPS advised him:

> *"Please note that multiple requests within a single item of correspondence are considered to be separate requests for the purpose of section 12. This means that there are three requests to be considered in this case. The MPS has decided to aggregate the total cost for all 3 requests by virtue of section 5 of the Fees Regulations, as they were received at the same time and relate to a similar overarching theme of the Counter Terrorism Internet Referral Unit (CTIRU) database"*.

39. Whilst the Commissioner accepts and agrees with this statement in isolation, the Fees Regulations do not specifically apply to section 14 of the FOIA so are not directly relevant. However, when considering burdensome requests, the Commissioner does accept that the general principle of costs where they relate to tasks which cannot be considered when applying the appropriate limit, may be relevant when considering the effect of burden.

40. The Commissioner has therefore necessarily considered each request in isolation when making her determination, and whether or not it is vexatious. However, she recognises the further cumulative burden caused by the three requests being submitted in succession, on the same day.

41. In the Commissioner's view, section 14(1) of the FOIA is designed to protect public authorities by allowing them to refuse requests which have the potential to impose a disproportionate or unjustified level of burden, disruption, irritation or distress. Balancing the impact of a

request against its purpose and value can help to determine whether the effect on the public authority would be disproportionate.

42. The actual purpose behind these requests is not known and the complainant has not offered any arguments as to why the information should be in the public domain. He has advised why he doesn't accept that his requests present an oppressive burden, and also why he does not consider that disclosure of the information would be in any way harmful, but he has not explained what public interest disclosure would serve and the Commissioner can see no obvious purpose other than that of general transparency.

Were the requests vexatious?

43. The Commissioner has considered both the complainant's position and the MPS's arguments regarding the information requests in this case. In reaching a decision she has balanced the purpose and value of the requests (as she has determined them) against the detrimental effect on the MPS of responding to them.

44. The sheer volume of information is particularly significant. The MPS provided the Commissioner with the figures caught by the scope of these requests, which are as follows:

> *"In respect of part (1) of the request, from 1 January 2018 until the time of the request the CTIRU database contains details of 11,413 investigations (DB1) and 26,009 URLs (DB2). In respect of parts (2) and (3) of the request, from 1 January 2020 to 1 April 2020 the database contains details of 855 investigations (DB1) and 2,398 URLs (DB2)".*

45. The complainant has argued that URLs could be disclosed as they have been removed from the internet and, in his view, there can therefore be no further harm. However, each URL would need to be checked prior to its disclosure to check that there is no 'live' link available - as the MPS has explained to the complainant, although a platform provider may have been requested to remove a link, it may be that this has not actually been done. The MPS would also need to verify whether or not each URL is part of any further related police investigation. This would involve an inordinate amount of work in assessing whether disclosure could have any further impact. Furthermore, even if a URL is 'dead' then the actual address may contain useful policing information.

46. The Commissioner accepts that the MPS would need to check all of the identified database entries prior to disclosure for each separate request. The data requested in each one (such as URL, content title, evidential capture, digital files) is gathered and recorded for a policing purpose and

may well be required for ongoing (or future) criminal investigations; it would not be possible to ascertain this without considering each entry.

47. Additionally, it is of considerable note that the database holds content that has been identified as needing removal from the public gaze. This request seeks to reintroduce into the public domain that very same information which the MPS has sought to remove. This would undermine the whole purpose of identifying and removing illegal content in the first place. The Commissioner considers that the reintroduction of such information into the public domain via the FOIA would weigh heavily against any perceived public interest in disclosure.

48. Based on the cogent evidence provided by the MPS, and the considerable harm that could be caused by reintroduction of the withheld information into the public domain, the Commissioner finds each of the requests to be vexatious. The MPS was therefore entitled to rely on section 14 of the FOIA to refuse the requests.

Right of appeal

49. 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

50. 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.

51. 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