

Freedom of Information Act 2000 (FOIA)

Decision notice

Date: 22 January 2024

Public Authority: Cabinet Office
Address: 70 Whitehall
London, SW1A 2AS

Decision (including any steps ordered)

1. The complainant has requested the Cabinet Office (CO) to disclose the video thumbnails and the first frame of all videos (including CCTV footage) that was provided to the Metropolitan Police in relation to its inquiry into breaches of Covid regulations. CO refused to confirm or deny holding the requested information in accordance with sections 31(3), 38(2) and 24(2) of FOIA.
2. The Commissioner's decision is that CO is not entitled to refuse to confirm or deny holding the requested information under sections 31(3), 38(2) and 24(2) of FOIA. He has also found CO in breach of section 10 of FOIA for failing to respond to the request within 20 working days of receipt.
3. The Commissioner requires CO to take the following steps to ensure compliance with the legislation.
 - Confirm or deny whether the requested information is held.
 - If information is held, it should either be disclosed or CO should issue a fresh refusal notice in compliance with section 17 FOIA.

4. The public authority must take these steps within 35 calendar days of the date of this decision notice. Failure to comply may result in the Commissioner making written certification of this fact to the High Court pursuant to section 54 of the Act and may be dealt with as a contempt of court.

Request and response

5. On 19 May 2022, the complainant wrote to CO and requested information in the following terms:
 - “1. Please provide me with copies of the video "thumbnails" for all of the videos (including CCTV footage) that were provided to the Metropolitan Police in relation to its inquiry into breaches of Covid regulations.
 2. Please provide me with the first frame of every video (including CCTV footage) that was provided to the Metropolitan Police in relation to its inquiry into breaches of Covid regulations.

In all cases, please blur out the faces of any individuals who can be identified within the images in accordance with data protection laws.”
6. CO responded on 28 July 2022. It refused to confirm or deny holding the requested information citing section 31(3) of FOIA.
7. The complainant requested an internal review on 11 August 2022. They said CO is unable to refuse to confirm or deny holding the requested information, as it is already publicly confirmed. They advised that if CO provided CCTV footage to the police, it stands to reason that it must hold the thumbnail and the first frames of each video.
8. CO carried out an internal review and notified the complainant of its findings on 24 November 2022. It upheld its application of section 31(3) of FOIA and advised that it also wished to rely on sections 24(2) and 38(2) to refuse to confirm or deny whether or not the requested information is held.

Scope of the case

9. The complainant first contacted the Commissioner on 28 October 2022 to complain about the way their request for information had been handled. At this time CO had not completed the complainant's request for an internal review. The Commissioner wrote to CO on 4 November 2022 to request that it complete this process within 10 working days. It

failed to meet this deadline, so on 22 November 2022 the Commissioner accepted the complaint for full investigation. The internal review response was then issued a couple of days later on 24 November 2022.

10. The Commissioner considers that the scope of his investigation is to establish whether or not CO is entitled to refuse to confirm or deny holding the requested information in accordance with sections 24(2), 31(3) and 38(2) of FOIA. He will first consider section 31(3), as this exemption was first cited. If he finds this does not apply, he will then go on to consider sections 24(2) and 38(2) as necessary.

Reasons for decision

Neither confirm nor deny (NCND)

11. Section 1(1)(a) of FOIA requires a public authority to inform a requester whether it holds the information specified in the request.
12. The decision to use an NCND response will not be affected by whether a public authority does, or does not, in fact hold the requested information. The starting point, and main focus for NCND in most cases, will be theoretical considerations about the consequences of confirming or denying whether or not a particular type of information is held.
13. A public authority will need to use the NCND response consistently, over a series of requests, regardless of whether or not it holds the requested information. This is to prevent refusing to confirm or deny being taken by requesters as an indication of whether or not information is in fact held.
14. CO had taken the position of neither confirming or denying whether it holds the requested information. The issue that the Commissioner has to consider is not one of disclosure of any requested information that may be held, it is solely, whether or not CO is entitled to NCND it holds any information of the type requested by the complainant.
15. During the Commissioner's investigation it was discussed with CO whether or not it considered the former Second Permanent Secretary's update on 31 January 2022¹ brought into question its ability to rely on

¹ [Investigation into alleged gatherings on government premises during Covid restrictions: Update \(publishing.service.gov.uk\)](https://publishing.service.gov.uk)

the NCND provision of the three exemptions cited. Paragraph 7 for example, which stated:

"We carried out interviews of over 70 individuals, some more than once, and examined relevant documentary and digital information, such as emails; Whatsapp messages; text messages; photographs and building entry and exit logs. This has also included searches of official records."

16. Although video footage, including CCTV, is not explicitly mentioned, the Commissioner thought it was reasonable to assume that CCTV would be in operation at 10 Downing Street and Whitehall, and if held, it would have been consulted and passed over to the Metropolitan Police Service (MPS).
17. CO advised the Commissioner that while it is correct to say that there is information that predates the request in the public domain which confirms that it holds evidence gathered as part of an investigation that was subsequently passed to the MPS, this update does not confirm that videos, including CCTV footage, were gathered by the former Second Permanent Secretary's investigation, nor that videos were passed to the MPS. It therefore considers the January update does not undermine its ability to apply the NCND provision of each exemption cited, as it makes no reference to the type of material stated in the request.
18. Additionally, CO referred to the update from the MPS on 19 May 2022 (which was published a few hours before the request was sent) and said that this also does not undermine its position. It confirmed that the update said:

"A team of twelve detectives worked through 345 documents, including emails, door logs, diary entries and witness statements, 510 photographs and CCTV images and 204 questionnaires as part of a careful and thorough enquiry."

It stated that while this update confirms that the MPS reviewed "CCTV images", it does not confirm that it reviewed videos per se, nor importantly, the source of those CCTV images (i.e. whether they were received from CO or another source).

19. Since these discussions the Commissioner has found a further update², which was published by the MPS on 31 January 2022. This confirmed

² [Update - investigation into alleged Covid breaches in Downing Street and Whitehall | Metropolitan Police](#)

that the MPS received the documentation from CO on 28 January 2022 and how it was:

"...now reviewing it at pace to confirm which individuals will need to be contacted for their account. This prioritisation will include reviewing all the material from the Cabinet Office, which includes more than 300 images and over 500 pages of information."

20. Although this quote does not directly tally up with the figures that were later quoted in May 2022, both highlight the extent of the information shared and how this included a substantial amount of "images".

Section 31(3)

21. Section 31 states that information is exempt from disclosure if its disclosure would or would be likely to prejudice any of the matters listed in subsection (1) or the exercise of any of the public authority's functions mentioned in subsection (2), by virtue of subsection (1)(g).
22. Subsection (3) confirms that the duty to confirm or deny does not arise if, or to the extent that, that confirmation or denial would or would be likely to prejudice the matters listed in subsection (1).
23. CO has cited section 31(2)(b) by virtue of 31(1)(g) in this case, stating that to confirm or deny holding the information would be likely to prejudice its ability to ascertain whether any person is responsible for any conduct that is improper. It said that it considers this includes the conduct which falls below standards of proper conduct set for public office holders, MPs, ministers or civil servants as set out by the ministerial, special adviser and civil service codes.
24. CO argued that confirming or denying whether it holds the requested information would undermine the effectiveness and the integrity of its investigation process, which is maintained by the understanding among those who participate in it that the fact of providing any information to the CO investigation, and the information itself, is kept in confidence. It said that it is vital that participants provide their information freely and openly and in an environment where they can trust that the fact that they provided information to the CO investigation, and the information provided, will not be disclosed. A confirmation or denial would make it possible to assume the identity of individuals who have provided information to the CO investigation.
25. The Commissioner considers a distinction should be drawn between any video footage that could have been supplied by witnesses or participants assisting the investigation (for example footage filmed on a phone) and CO's own CCTV if indeed held. The former would be information shared freely and openly for the purposes of the investigation and on a

confidential basis. If held and we were considering disclosure, the Commissioner could see the argument here that CO is making. However, any CCTV footage (if held and was being considered for disclosure) would not. This would be CO's own information it would obtain itself for the purposes of the investigation, not information volunteered to CO by those asked or instructed to assist with its enquiries.

26. We are also not considering the disclosure of any information held (if indeed it is), we are considering whether CO should confirm or deny holding any information of the nature described in the request under FOIA. In other words, the simple existence or not of the information and whether saying it is held or not would or would likely prejudice CO's ability to carry out such investigations.
27. From the submissions received, the Commissioner is unconvinced that confirming or denying the information is held would or would be likely to have the effects CO has described. Disclosing whether or not it holds such footage would not in itself disclose the contents of any footage held or reveal its source. If CCTV images are held, these would be CO's own information; not information it had obtained from a witness or participant in the investigation. If other footage is held, confirming that it is, would not be likely to prejudice the confidential nature of CO's investigation process nor the ability or cooperation of those it needs to assist with that investigation. Simple confirmation would not reveal the source or any details about the contents of that footage and the Commissioner considers it would need to be this sort of information which is gained from CO's response to a request, which could then be argued to have the effects it has described on its law enforcement functions.
28. The Commissioner also considers that the MPS confirmed publicly on 31 January 2022 that it received over 300 images from CO for the purposes of its own enquiries. The Commissioner accepts that the use of the word "images" does not confirm the nature of those images (whether photographs, video footage or CCTV) but he does consider this information, taken with the MPS' later quote on 19 May 2022 when it is confirmed that it looked at CCTV images (although no source mentioned here), brings into question the validity of CO's position to refuse to confirm or deny holding the information.
29. It is important to stress that the Commissioner himself does not know if any information of the nature specified in the request is held or not, as this would undermine the purpose of the NCND provision under FOIA. The above comments and reasoning are based on the submissions received from CO and what is or is said to be in the public domain.

30. For the above reasons, the Commissioner has concluded that CO is not entitled to rely on section 31(3) of FOIA.

Section 38(2) Health and Safety

31. Information is exempt from disclosure under this exemption if its disclosure would or would be likely to endanger the physical health of any individual or endanger the safety of any individual. Subsection (2) states that the duty to confirm or deny does not arise if, or to any extent that, that confirmation or denial itself would or would be likely to have either of these effects.
32. CO confirmed that confirming or denying if the requested information is held could allow external actors to build an understanding of the retention policies and practices for CCTV footage, thereby threatening the physical security of its buildings and the personal security of those that use them.
33. It advised that by confirming or denying whether CCTV footage was retained for a certain period, CO would be revealing sensitive information about its retention policies which would, in turn, affect the physical safety of 10 Downing Street. This location and CO are high profile government sites which hold information important to national security, as well as the personal security of staff members and the Prime Minister and family.
34. CO said linked to this, it needs to consider the consequences of routinely confirming or denying whether CCTV footage was held for certain dates. Such confirmation or denial entering the public domain would allow a hostile actor to piece together information about its retention policy to the extent that they may be able to then threaten the physical security of these government offices.
35. It went on to say that there is a causal relationship between confirming or denying whether CO holds the information in the scope of the request and endangerment to the physical health of those who work in the buildings. It argued that given the seriousness of the implications of a breach of physical security of these buildings, which would be aided by building up a detailed understanding of the CCTV retention practices, it considers that such a breach would have a detrimental effect on the wellbeing of those working in those buildings.
36. Again the Commissioner would point out that the request asked for video footage, including CCTV, it was not just for CCTV footage. Confirming or denying whether the requested information is held would therefore not be confirming or denying holding a particular type of footage; just that it holds live footage the source of which is not known.

37. Confirming or denying holding the requested information would not disclose anything definitive in this particular case in relation to CO's retention policies or procedures for CCTV. CO's investigation looked into a number of events over an 11 month period (May 2020 and April 2021) with the latest event being 16 April 2021 just short of 8 months prior to the Prime Minister's instruction to the Cabinet Secretary to carry out an investigation. Confirmation or denial would only be confirming whether or not video footage relating to any one of those events is still held.
38. If CO is using the mosaic argument and consistency approach here (saying that if a consistent approach is not taken to requests relating to CCTV it would be possible for a member of the public to build up information relating to its retention policies and procedures over time by asking about specific events, dates or times) the Commissioner considers for this particular request those arguments are a little too far removed. There were several events covered by the investigation, the request was not limited to just CCTV and any confirmation or denial would not be revealing anything definitive about those retention policies or procedures that could be then used to compromise the security of its buildings and therefore potentially endanger the physical health or safety of an individual. Confirmation or denial does not disclose any information on the location or angles of any CCTV and the Commissioner believes it is this type of information, if disclosed, that would be likely to have the effects CO has described.
39. Going back to the Commissioner's arguments in paragraph 28 above, he considers these are equally applicable here. The information in the public domain does bring into doubt the validity of CO's position to refuse to confirm or deny holding the information.
40. The Commissioner has therefore concluded that CO is not entitled to rely on section 38(2) of FOIA.

Section 24(2) National security

41. Section 24(2) provides an exemption from the duty to confirm or deny whether information is held, where the exemption is required for the purposes of safeguarding national security.
42. CO argued in this case, the risk to national security comes from confirming or denying details about the physical security of 10 Downing Street and CO – the home and workplace of the Prime Minister i.e. whether and for how long CCTV footage is retained by the government. It said that the rationale for the application of this exemption and its refusal to confirm or deny is very similar to that for section 38(2), as detailed above.

43. It confirmed that confirming or denying whether this information is held would damage national security by revealing sensitive information about what security arrangements may or may not be in place within a high profile government building, including insight into what information may, or may not, be stored. This could be used by anyone wishing to analyse or circumvent security measures.
44. Again, the Commissioner's arguments on what information is already in the public domain and how the request not only covers CCTV but all video footage equally apply here.
45. Additionally, similarly to section 38(2) the Commissioner remains unconvinced that confirming or denying whether the requested information is held is required to protect national security. It would not reveal anything definitive about retention policies or procedures or disclose any sensitive information about the location or angles of any CCTV, which could then be used to threaten national security. The Commissioner considers it is the latter information which could be potentially used to threaten security but this information would not be revealed from a simple confirmation or denial in this case.
46. Again, based on the submissions CO has presented, the Commissioner is not persuaded that CO is entitled to rely on section 24(2) of FOIA.
47. The Commissioner would like to highlight here that although he has reached the conclusion that CO cannot rely on the NCND provision of the exemptions it has cited for this particular request because it has failed to make that case, this decision does not set a precedent for any future requests it may receive in relation to video footage, including CCTV. Each and every request must be considered on its own merits based on the particular information requested, the circumstances at the time of the request and what confirmation or denial (or disclosure if this is being considered) would reveal.
48. As the Commissioner has found that none of the NCND exemptions apply, there is no need to go on to consider the public interest test.

Procedural matters

49. Section 10 of FOIA requires a public authority to respond to an information request promptly and in any event no later than 20 working days from receipt. The request was made by email on 19 May 2022 and CO responded on 28 July 2022. CO exceed the statutory timeframe for compliance and therefore breached section 10 of FOIA.

Other matters

50. The section 45 code of practice requires public authorities to carry out an internal review within 20 working days of receipt, and certainly no later than 40 working days from receipt. The additional 20 working days should only be required in the most complex and voluminous of requests. In this case the request for internal review was made on 11 August 2022 and CO took until 24 November 2022 to issue its response.

Right of appeal

51. 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

52. 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.
53. 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

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