

Freedom of Information Act 2000 (FOIA)

Decision notice

Date: 7 November 2022

Public Authority: House of Commons
Address: Westminster
London
SW1A 0AA

Decision (including any steps ordered)

1. The complainant requested from the House of Commons (HoC) information relating to blocked website categories accessible in the HoC. The HoC provided information to some parts of the request but withheld information to the remaining parts and cited section 31(1)(a) (law enforcement) and section 24(1) (national security) of FOIA.
2. The Commissioner's decision is that the HoC was entitled to withhold the information to request 1 under section 31(1)(a) of FOIA. Also, the public interest in maintaining the exception outweighs the public interest in disclosure. The Commissioner does not require the HoC to take any steps as a result of this decision.

Request and response

3. On 27 April 2022 the complainant wrote to the HoC and requested information in the following terms:

"FoI request 1 of 3

From relevant documentation, please provide a copy of what website categories are blocked on the Wi-Fi internet accessible in the House of Commons (e.g. gambling, hate speech, porn).

FoI request 2 of 3

Kindly confirm existence of a system in place to help prevent (or deter) MPs from watching porn on their phones inside the House of Commons chamber.

FoI request 3 of 3

From records, please indicate who is responsible for ensuring MPs do not watch pornography while in the House of Commons.

For public reference: A Tory MP was recently caught watching pornography on his phone while in the House of Commons <https://www.facebook.com/stopuklies/phot...>

4. On 23 May 2022 the HoC provided its response and confirmed it holds a breakdown of website categories blocked on the parliamentary network. The HoC however, withheld the requested information to request 1 by virtue of both section 31(1)(a) (law enforcement) and section 24(1) (national security) FOIA. The HoC provided the complainant with a copy of two decision notices in order to support its position on details of disclosure of this information. With regard to request 2, the HoC provided confirmation, and to request 3 the HoC stated information is not held.
5. The complainant asked the HoC for an internal review. She considered the decision notices which it provided and had relied upon to support its position are "very different" to what she requested. The complainant argued that her request is more general and does not involve specific lists of websites accessed. She said the information requested in the decision notices, is specific and she agreed it would have implications if released. The complainant clarified her request is for "categories of website that were blocked from being accessed."
6. The complainant argued that the provision of such categories would not aid cyberterrorism or prevent crime from being detected or cause a security breach. She said "security breaches are inbound in nature, not outbound."
7. With regard to request 2, the complainant accepted the HoC response explaining the outbound blocking system which it has in place. The complainant therefore withdrew request 2 but said she is still seeking information to the remaining requests.
8. The HoC provided its internal review response on 27 June 2022, and maintained its original position to withhold some of the information under the exemptions cited.

9. The complainant did not accept that information to request 1 is exempt from disclosure. She clarified she would be content with confirmation from the HoC that there is a record showing the category of pornography is blocked on the Wi-Fi internet accessible in the HoC. The complainant added she accepts that "category blocks are not full proof."
10. In response to the complainant's correspondence, the HoC stated it has nothing further to add to the responses it has already provided, and reiterated the complainant's right to complain to the ICO.
11. As the complainant subsequently withdrew request 2 (paragraph 7) and the HoC responded to request 3, the following analysis focuses on whether the exemption at sections 31(1)(a) and 24(1) of FOIA were cited correctly to request 1.

Reasons for decision

Section 31 – law enforcement

12. Section 31(1)(a) of FOIA states that:

"Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice -

(a) the prevention or detection of crime,"

13. The HoC confirmed that it holds a breakdown of website categories blocked on the parliamentary network. It stated that disclosure of the information requested would assist those with criminal or malicious intent to circumvent its blocking measures. HoC explained that this would be likely to prejudice the prevention or detection of crime, the apprehension of offenders and could also undermine the safeguarding of national security.
14. In response to requests about websites accessed within Parliament, the HoC directed the complainant to previous decision notices regarding the use of the exemptions it cited. The HoC said that these notices (although not identical to the complainant's request) involve similar general principles and risks.

15. The HoC responded to request 3, it said that information to this is not held by the HoC because there is no sole person or team responsible for ensuring this within the HoC Administration. The HoC provided the complainant with details of various disciplinary routes and procedures regarding misconduct of Members, both internal to the House and externally via their respective parties.
16. The HoC explained that there is an acceptable use policy for the Parliamentary Network and it provided the complainant with a redacted copy of the policy. The HoC said that the existence of such a policy does not ensure MPs are unable to watch pornography in the HoC, but it does contribute to an environment in which there are technical and behavioural impediments to doing so. The HoC added that the software and disciplinary routes and procedures also contribute to this environment. The HoC informed the complainant of the person responsible for the acceptable use policy, and the software which is the Managing Director of the Parliamentary Digital Service – David Smith.
17. The Commissioner considers that, in the HoC responses to the complainant, the HoC has satisfied all three stages of the prejudice test set out on Hogan and therefore accepts that section 31(1)(a) is engaged. He finds that the chance of prejudice being suffered from disclosure of the requested information is more than a hypothetical possibility; it is a real and significant risk.

Public interest test

18. Section 31(1) is a qualified exemption and is therefore subject to the public interest test set out in section 2(2)(b) of FOIA. The Commissioner has considered whether in all the circumstances of this case, the public interest in maintaining the exemption outweighs the public interest in disclosing the withheld information.

Public interest arguments in favour of disclosure

19. The HoC accepts that in these matters, the legitimate public interest is being open and transparent so that the public can have confidence in the way the HoC operates. It said, there is a public interest that individuals that use the parliamentary network to access the internet, should be able to do so securely. However, the public also need to be assured that these taxpayer funded resources are being used in a way that is appropriate to the work of the HoC.
20. The complainant said disclosure of the information requested would allow the public to see "work has been done to try and prevent access to this kind of material, and that the users of this network cannot simply do whatever they please on taxpayers time in the area of the HoC."

Public interest arguments in favour of maintaining the exemption

21. The HoC explained that disclosure of this information would assist cyber criminals looking to circumvent Parliament's security systems. Disclosing details of blocked categories would allow cyber criminals to determine which sites or site categories were unfiltered. Therefore, this would aid their ability to launch for a potential cyberattack against the HoC servers. The HoC said that in particular, it would leave the Parliamentary Network exposed to a number of potential cyber security issues. This includes, but not limited to, water-holing, phishing, domain squatting, loss of personal data and similar types of attack. In the case of water-holing, rather than attempting to breach the security of the parliamentary network, the HoC said an individual could target the network users by aiming their malicious code or activities at other website categories that they know are being visited. This would mean the HoC would fail in its duty to help prevent criminal attacks on its network. The HoC would then fail in its duty to help prevent criminal attacks on its network and fail in its duty to assist those services providing it with law enforcement. As a result, the HoC consider that this would prejudice the prevention and detection of crime.

Balance of the public interest arguments

22. The Commissioner acknowledges there is a strong public interest in reassurance, and that a public authority has appropriate measures to mitigate potential cybercrime. The Commissioner considers disclosure of the withheld information would reduce this level of reassurance, this is because criminals would be more aware of which category of websites they could target where a public authority may be more vulnerable. This would reduce public confidence in the HoC ability to alleviate potential cybercrime.
23. Having considered the arguments from both parties, the Commissioner is satisfied that disclosure of the information at request 1 would be likely to prejudice the prevention or detection of crime. Therefore, section 31(1)(a) of FOIA is engaged.

The Commissioner's position

24. The Commissioner agrees there is a public interest in openness and transparency. Release of the information would provide the public some reassurance the HoC are limiting the use of inappropriate material being accessed in the HoC. The Commissioner also acknowledges that it is not a request for specific lists of websites accessed or anything actually accessed.

25. However, the Commissioner considers there is greater public interest in preventing potential cybercrime on the HoC security systems, which provides the public confidence that the HoC has appropriate measures in place to handle cybercrime.
26. The Commissioner determines that release of the withheld information would provide motivated cyber criminals the ability to target categories of websites that the HoC does not block. This would reduce public confidence in the HoC ability to prevent cybercrime. The Commissioner therefore considers the arguments for withholding the information outweighs the arguments in favour of disclosure.
27. The Commissioner concludes that the HoC was entitled to withhold the information at request 1 under section 31(1)(a) of FOIA. As the exemption is engaged, the Commissioner is not required to consider the HoC reliance on section 24(1) of FOIA to withhold the requested information.

Right of appeal

28. 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: 0300 1234504

Fax: 0870 739 5836

Email: grc@justice.gov.uk.

Website: www.justice.gov.uk/tribunals/general-regulatory-chamber

29. 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.
30. 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

Phillip Angell
Group Manager
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF