Freedom of Information Act 2000 (FOIA)

Decision notice

Date: **28 April 2020**

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

Decision (including any steps ordered)

1. The complainant has requested from the House of Commons ("HoC") information on specified websites accessed from the parliamentary network. The HoC relied on Section 31 (law enforcement) and Section 24 (national security) to withhold some of the requested information and denied holding the remainder.

2. The Commissioner's decision is that the HoC correctly relied on section 31 to withhold the requested information that it held and did not hold the remaining requested information.

3. The Commissioner does not require the public authority to take any steps.

Request and response

4. On 3 December 2018, the complainant wrote to the HoC and requested information in the following terms:

   Request 1

   Since the start of 2018, all websites accessed from parliamentary network with the top-level domain .xxx or .porn and the number of times they were accessed.

   Request 2

Since the start of 2018, all websites accessed from the parliamentary network with the words or word fragments 'porn', 'teen', 'tube', 'xxx', 'hamster' and the number of times they were accessed.

5. On 19 December 2018 the HoC responded, saying as follows:

Request 1

It refused to provide the requested information. It cited the following exemptions as its basis for doing so:

- Section 31 (law enforcement)
- Section 24 (national security)

Request 2

It denied holding this requested information.

6. The complainant requested an internal review on 19 December 2018. The HoC sent him the outcome of its internal review on 22 January 2019. It upheld its original position.

Scope of the case

7. The complainant contacted the Commissioner on 22 January 2019 to complain about the way his request for information had been handled.

Reasons for decision

Request 1

8. Section 31(1)(a) 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,"

HoC's submissions

9. In addition to the below submissions, there are further (considered) submissions, from the HoC which due to their sensitivity are contained in a confidential annex. A copy of this annex will be shared with the HoC but not with the complainant.

10. It is well recognised that criminals use the internet to target individuals and to carry out criminal activity. A list of the requested websites accessed from the Parliamentary network would be useful in a variety of ways to those who wish to carry out criminal activities.

    For example:

    • The list could enable "water-holing": rather than attempting to breach the security of its network, an individual could target its network users by aiming their malicious code or activities at other websites. For example, by finding a website which is popular, and yet run by an individual or a small organisation without the resources to invest in robust cyber-security measures, users of its network can be targeted (as laid out immediately below) by aiming activities at that website.

    • Having learned which websites are most likely to yield results from its network users, a criminal could then use "domain squatting" or "cyber-squatting": i.e. taking over that site, or assuming its identity. In this example, network users may believe that they are accessing the genuine site but they are in fact communicating with the false (or "spoof") site, thereby potentially allowing their data to be obtained by an unknown person. This data includes, home addresses, names and date of birth. Depending on the context of the false website, individuals could be asked for credit card or passport details, for example. Attackers can also obtain corporate data such as email addresses - perhaps believing they are updating a subscription to a mailing list; or usernames and passwords – believing that they are logging into a site that they regularly use. It is possible for their communications to be redirected to the genuine site, after their data has been obtained, while they remain unaware that their communications had been intercepted.

    •Request metrics can also be used to measure the success of a "phishing attack" (where individuals are tricked into replying or responding to emails, thereby providing data or enabling infection by a virus or other "malware") and therefore improve the effectiveness of further attacks. This is done by infecting a control server elsewhere and then having the malware call back to that domain or IP address - this can often be a problem in cases of "hijacked domains" or where misdirection is used on an infected website.

    •An attacker could also launch a malicious website with a similar name to others on the retrieved list – in the "trade" this is known as typo squatting and poses risks usually relating to theft of personal data.

11. The HoC also believe that disclosing this type of information (including the number of times websites were accessed) would give an attacker information on its filtering policy, its blocking policy and potentially the technology it uses in this area:

•An attacker might have requested information to ascertain if a particular site had been picked up and categorised by the filtering software. An attacker could ask again for a repeat snapshot of data later and work out how long it takes to block a site and what the window of opportunity for an attack might be.

•An attacker might set up a malicious site and want to ascertain whether it has been blocked or not.

• An attacker could potentially work out which filtering product it relies on from results retrieved. There are only a limited number of filtering products on the market and they all operate in slightly different ways with their own vulnerabilities. It is therefore important to protect its choice of product.

Commissioner's analysis

12. In order for a prejudice based exemption, such as section 31(1), to be engaged, three criteria must be met:

- 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. In relation to the lower threshold the Commissioner considers that the chance of prejudice occurring must be more than a hypothetical possibility; rather there must be a real and significant risk. With regard to the higher threshold, in the Commissioner's view this places a stronger evidential burden on the public authority. The anticipated prejudice must be more likely than not.

13. The Commissioner accepts that the potential prejudice described by the HoC clearly relates to the interests which the exemption contained at section 31(1)(a) is designed to protect. That is the criminal harm, the HoC alleges would be likely to occur if the withheld information was released, relates to the prejudicing of the prevention or detection of crime.

14. With regard to the second criterion, the Commissioner acknowledges that the threat from cyber-attacks that the HoC faces (as they are for the public and other bodies) are clearly real ones. The reality is that cybercrime is a clear and continuing danger in contemporary society. As a result the Commissioner accepts that it is persuasive to argue that there is likely to be a causal link between disclosure of the information and prejudice occurring. That is, releasing the withheld information likely would aid those who would commit criminal acts against the HoC computer networks. In this context releasing the withheld information would be a release to the whole world, including the most sophisticated (state) actors. Accordingly it would mean that a suite of information, with all its possible dangers (both known and unknown), is placed in the hands of the most adroitly skilled "hackers".

15. Consequently the Commissioner accepts that any such resultant prejudice if the withheld information is to be disclosed is real, actual and of substance.

16. With regard to the third criterion, the Commissioner is satisfied that if the withheld information was disclosed there is a more than a hypothetical possibility that prejudice of the nature envisaged by the HoC would be likely to occur. The exemption contained at section 31(1)(a) is therefore engaged.

Public interest test

17. Section 31(1) is a qualified exemption and therefore subject to the public interest test set out in section 2(2)(b) of FOIA.

18. The Commissioner has therefore considered whether in all the circumstances of the case the public interest in maintaining the exemption outweighs the public interest in disclosing the withheld information. The Commissioner has received public interest arguments from the HoC but not the complainant. The Commissioner found the public interest arguments from the HoC compelling, worthy of adopting and are replicated below:

19. The HoC acknowledged the fact that there is a legitimate public interest in being reassured that computers are being used to visit websites that are secure and appropriate to its the work. Equipment and the network are provided at public expense and many of the network users are public servants. The HoC also acknowledged that is a valid concern to ensure that the House and those who are associated with it carry out their business in a proper manner, including the use of its network to access the internet.

20. However, the HoC argued that the public interest in preventing a cyber attack against its network or against others who may be affected as a result of disclosure, and the public interest in ensuring that data which is

processed by the national UK legislature is seen to be processed properly and securely, outweighs the arguments in favour of disclosure.

21. The HoC also argued that it had a legal duty under data protection legislation to safeguard the parliamentary network. In doing so, it protects the operation of the HoC itself, the security of the vast quantity of data (including personal data about network users and about members of the public) which the network deals with and also the cyber security of the individuals who use the network. It is also vitally important that information about the use of the network is not used against other websites or against individuals.

22. The Commissioner's decision is that the public interest in preventing a cyber-attack against the HoC's network or against others who may be affected as a result of disclosure, and the public interest in ensuring that data which is processed by the national UK legislature is seen to be processed properly and securely, outweighs the arguments in favour of disclosure.

23. Accordingly, for the reasons given above, the Commissioner has come to the conclusion that the HoC correctly relied on section 31(1)(a) to withhold the requested information.

Request 2

24. The HoC maintains that it is does not hold this requested information. In order to create this information, it would have to (it says) extract a list of all websites accessed from the log files and then search each site individually for the terms listed, a two-stage process. It has never run a report for this before (searching for truncated terms). The cumulative annual browsing history of Parliament equates to 9TB of data. It has no way of extracting, searching or storing this amount of data and has no business need to conduct this type of search.

25. In order to generate the requested information, it would need to produce the initial report and then access every external website on the list to search for those words or fragments. The second building block is therefore the entire contents of every external website on the list.

26. It has not carried out any search for the listed words, it has not downloaded any data and it has not printed anything off in response to this request. It has not entered into any licence agreement with these websites – this is purely information which is published by third parties online; it has no rights over the content and no control.

27. It accepts that a public authority can hold information which has been sourced online, if it has taken active steps such as downloading or printing the material. However, it cannot be correct that, simply because an external website has been accessed from its network, it therefore

holds all of the contents of that website. That premise would potentially impose a duty on all public authorities to carry out online research in response to any FOI request, if a relevant website had ever been accessed from their own network.

Commissioner's analysis

28. The Commissioner's guidance note[1] on "Determining whether information is held" states in the Overview section that;

"a public authority will hold information if it holds the building blocks required to generate it……" and "information that is available to a public authority online will only be held by that public authority if it has downloaded or printed it off".

29. In more detail, the Commissioner's guidance refers to the case of Glen Marlow -v- Information Commissioner (EA/2005/0031): in that case, the Tribunal decided that information in an online legal library was held if the public authority had selected it, downloaded and saved it or had printed it off. All of the other information within the database was not held. "Held" was therefore given the meaning of "an ordinary English word", as described in University of Newcastle upon Tyne -v- ICO and the British Union for the Abolition of Vivisection (GIA/194/2011) – without adding any technical or additional layers about potential for access, control or ownership.

30. On balance, the Commissioner have come to the conclusion that the HoC, on the balance of probabilities, does not hold this requested information, in that they do not physically hold a list of all websites visited where the words or word fragments 'porn', 'teen', 'tube', 'xxx', 'hamster' are to be found. The HoC is not expected or required (for the purposes of FOIA) to search all websites visited (from its computers) to determine and list the usage of the specified words. In essence, by way of reminder, FOIA gives a right to be provided with information actually held by a public authority.

31. The Commissioner did query, with the HoC, whether the complainant was merely is seeking the web addresses with the target words in the title and the number of times they were visited.

[1] https://ico.org.uk/media/for-organisations/documents/1169/determining_whether_information_is_held_foi_eir.pdf

32. The HoC explained it was entitled to interpret the request reasonably. While there may be other possible ways to interpret the request, that does not mean that its approach was unreasonable.

33. It pointed out, in this case that the requestor has used specific terms in his first request, so he is clearly well-informed on the subject. He had chosen to use a much broader description in his second request.

34. In addition, the "title" of a website is in itself a specific technical term. This term relates to the contents of the html reference for the website – for example, it would be what a search engine such as Google would display in its results. It is quite different again from the web address itself. It had enquired with its supplier and it understands that the web filtering software would not be able to produce a report using the title of websites.

35. This issue demonstrates how the scope of the request, the information that it holds and the practicalities of the search are all dependent on the question. It does not accept that the question in this case refers to the title of the websites and it repeated its position that the question should be interpreted as it has been written, especially where the requestor has shown that he has some technical knowledge on the subject.

36. The Commissioner considers that the HoC's interpretation of the request to be a reasonable and objective one, hence the Commissioner's decision in paragraphs 28 to 30 above. However even if the complainant was indeed seeking the number of pertinent websites with "fragments 'porn', 'teen', 'tube', 'xxx', 'hamster' and the number of times they were accessed" in the top level domain with the top-level domain then that information would be exempt as well, for the above reasons given for "Request 1" information.

Right of appeal

37. 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 123 4504
    Fax: 0870 739 5836
    Email: grc@justice.gov.uk
    Website: www.justice.gov.uk/tribunals/general-regulatory-chamber

38. 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.

39. 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 .....

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