Freedom of Information Act 2000 (FOIA)

Decision notice

Date: **28 March 2018**

Public Authority: Ministry of Justice

Decision (including any steps ordered)

1. The complainant has requested information in relation to the number, nature, and effects of cyber attacks on the Ministry of Justice. The department relied on the exclusion at section 31(3) FOIA as its basis for neither confirming nor denying whether it held information within the scope of the request.

2. The Commissioner's decision is that:

   - The Ministry of Justice was not entitled to neither confirm nor deny holding information within scope of the first part of the request.[1]

   - The Ministry of Justice was entitled to neither confirm nor deny whether it held information within the scope of the second part of the request.[2]

3. The Commissioner requires the public authority to take the following steps to ensure compliance with the legislation.

   - Confirm or deny whether it holds information within the scope of the first part of the request.

4. The Ministry of Justice 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

[1] The Commissioner has highlighted this as Part 1 of the request in the main body of this notice.

[2] The Commissioner has highlighted this as Part 2 of the request in the main body of this notice.

pursuant to section 54 of the Act and may be dealt with as a contempt of court.

Request and response

5. On 3 November 2016 the complainant wrote to The Ministry of Justice (MOJ) and requested information in the following terms:

"I write with a request for information about cyber attacks on the department….

Please disclose the number of recorded cyber attacks in 2015;

Please disclose the number of recorded cyber attacks to date in 2016;

For 2016, please provide:

A month-by-month breakdown;

The number of successful attacks – i.e. where there was a breach;

In the cases of a breach, please disclose:

the nature of the attack (DDOS, phishing etc),

the nature of the breach,

how many individuals' information were affected,

whether any classified information was affected,

what organisations or individual/s are suspected to known to have made the attack."

6. MOJ responded on 15 November 2016. It neither confirmed nor denied holding information within the description specified in the request by virtue of the provisions in section 31(3) (Law enforcement) FOIA.

7. Following an internal review the MOJ wrote to the complainant on 6 December 2016. The original decision to rely on section 31(3) was upheld.

Scope of the case

8. The complainant contacted the Commissioner on 8 December 2017 to complain about the way his request for information had been handled.

The Commissioner has referred to his submissions at the relevant parts of her analysis below.

9. The scope of the Commissioner's investigation therefore was to determine whether the public authority was entitled to neither confirm nor deny holding information within the scope of the request on the basis of section 31(3) FOIA.

Reasons for decision

10. For ease of reference, the Commissioner has divided the request into two parts. Part 1 covers the first part of the request for the number of recorded cyber attacks in 2015 and 2016. Part 2 covers the second part of the request for details about cyber attacks for 2016 including the number of attacks broken down by month, the nature, and the effects of those attacks.

Section 31(3)

11. MOJ has relied on this exemption on the basis that confirming or denying whether it holds information within the scope of the request would be likely to prejudice the prevention or detection of crime.

12. The relevant provisions in section 31 state:

> 1. 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……..
>
> 3. The duty to confirm or deny does not arise if, or to the extent that, compliance with section 1(1)(a) would, or would be likely to, prejudice any of the matters mentioned in subsection (1).

13. MOJ has argued that merely revealing whether or not the department had, or had not, detected a cyber-attack would significantly assist potential criminal activity if the information was used by malicious actors. Confirmation or denial that information is held would provide sufficient detail for malicious actors to highlight that some attacks, or certain types of attacks, were not noticed or recorded. This would expose the department's ICT systems to more attacks. If a malicious actor had carried out attacks it would appear that their attacks had gone undetected, indicating that the department did not have sufficient defences against cyber attacks. This could lead to malicious parties targeting future attacks against the department.

14. Furthermore, in line with recent guidance issued by the Cabinet Office, a neither confirm nor deny stance (NCND) needed to be applied consistently to protect departments who will not be in a position to confirm that information is held. In the absence of a consistent application of NCND, there is a real risk that responses from individual departments would impact on cross government cyber security. In response to the complainant, it acknowledged that the department was subject to a Distributed Denial of Service (DDOS) attack in 2014 as reported by Sky News. This brought down the department's website for a short period. The department therefore used media (twitter) to release a message stating its website was down due to a DDOS attack but that it was working hard to bring it back online as soon as possible. This message was released in order to assure users that work to bring the department's website back online was underway. MOJ however stressed that it does not routinely comment on cyber attacks launched against its ICT system because this would give malicious actors an unnecessary advantage.

15. With respect to the balance of the public interest, MOJ acknowledged that it was in the public interest to know that the department has measures in place to protect its information and be able to provide public services. It however argued that it was precisely for this reason that the department needs to do everything it can to limit the opportunities of malicious actors to identify any weaknesses or vulnerabilities in its ICT systems. Given that a cyber attack could have serious and potentially damaging consequences affecting court procedures, applications for legal aid, prison and probation services etc, there is a strong public interest in applying NCND to the request.

Complainant's position

16. The complainant's position is reproduced below.

"The neither confirm nor deny response itself is untenable. It is clear that MOJ does record cyber attacks. The Government has previously spoken about the many thousands of attacks on departments each month and other departments have previously confirmed attacks, including: http://news.sky.com/story/cyber-attack-on-ministry-of-justice-website-10417630

To be clear: the request is for * numbers of attacks * numbers of successful attacks and in those cases the type of attacks etc. There is a compelling public interest in disclosure of information capable of informing people how many attacks there have been and how many have been successful or not. Transparency allows the public to scrutinise whether the millions of pounds of public money being spent on secure systems is adequate and provides sufficiently robust protection for data

held by MOJ. Only recently the Government announced that £1.9 billion of public money is being spent on cyber security. This alone provides a compelling justification for transparency surrounding this issue.

It must also be pointed out that transparency will increase public confidence in Government security.

None of the information requested would help hackers. It doesn't reveal the hacks they used to penetrate the systems. It simply reveals how many attacks have been successful and how many people were affected etc.

There is a compelling and legitimate public interest in knowing how secure MOJ's systems are. Information concerning Britons relies on MOJ having resilient systems and it is paramount that the public is able to obtain basic information about how secure those systems are. It must be pointed out that the numbers are capable of demonstrating how many attacks have failed. This shows that public money MOJ has spent on secure systems has been well spent and, as mentioned, improves confidence in MOJ."

Commissioner's position

17. Including this complaint, the complainant submitted complaints against 13 departments in total pursuant to the same request under consideration in this case. In addition to MOJ's submissions in this case, the Commissioner has received a confidential submission from the Cabinet Office in support of reliance on NCND by 11 of the departments including MOJ. The remaining two departments have not relied on NCND.

18. For the avoidance of doubt, the Commissioner has considered all of the submissions received in this case including the complainant's above.

19. The duty imposed on public authorities to either confirm or deny whether they hold information of the description requested by an applicant is enshrined in section 1(1)(a) FOIA (commonly referred to as the duty to confirm or deny).

20. Part II of the FOIA contains a number of exclusions from the duty to confirm or deny. Section 31(3) FOIA is one of those exclusions from the duty to confirm or deny.

21. A public authority may withhold information on the basis of section 31(1)(a) if its disclosure would be likely to prejudice the prevention or detection of crime. Section 31(3) is available to a public authority if it considers that compliance with the duty in section 1(1)(a) would be likely to prejudice the prevention or detection of crime.

22. Clearly, exclusions from the duty to confirm or deny and exemptions from compliance with the requirement in section 1(1)(b)[3] cannot be relied on simultaneously in response to the same request.

23. Therefore, the question for the Commissioner with respect to the application of section 31(3) is whether confirming or denying information is held within the scope of the request would be likely to prejudice the prevention or detection of crime. In other words, would compliance with the duty to confirm or deny pose a real and significant risk of prejudice to the prevention or detection of crime?

24. The complainant has noted that MOJ responded to a specific cyber attack in 2014. MOJ has acknowledged that the attack resulted in a denial of service to users which prompted the department to publish a message assuring users that work was underway to restore services. The Commissioner does not consider that this undermines MOJ's argument for relying on NCND in order to protect its ICT networks especially internal networks against which threats and attacks may not always be apparent to the public.

25. Nevertheless, there is sufficient other information in the public domain in the Commissioner's view which at least suggests that as a government department, it is more probable than not that it has been the subject of cyber attacks. For example, on 1 November 2016 the Chancellor of the Exchequer published the National Cyber Security Strategy 2016-2021 which contains the following statement: "We regularly see attempts by states and state-sponsored groups to penetrate UK networks for political, diplomatic, technological, commercial and strategic advantage, with a principal focus on the government, defence, finance, energy and telecommunications sectors."[4] Furthermore, in a speech given at the Billington Cyber Security Summit on 13 September 2016 by the Chief Executive of the National Cyber Security Centre (NCSC) he stated, "….last year we detected twice as many national security level cyber incidents – 200 per month – than we did the year before."[5]

---

[3] To release requested information to an applicant.

[4] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

[5] https://www.ncsc.gov.uk/news/new-approach-cyber-security-uk

26. Therefore, in the Commissioner's view the prejudicial effect of issuing a response which effectively confirms or denies whether there were recorded incidents of cyber attacks at MOJ in 2015 and 2016 would be minimal. Revelatory public pronouncements at such high levels of government undermine the view that confirming or denying whether these attacks occurred would pose a real and significant risk of prejudice to the prevention or detection of crime. The Commissioner has also considered the confidential submission by the Cabinet Office and has concluded that it supports her position in the circumstances of this case. She has explained the rationale for this conclusion in a confidential annex.

27. However, the Commissioner considers that MOJ's response to the second part of the request for a detailed breakdown of the number of cyber attacks, the nature, and effects of the attacks is likely to be more useful to malicious actors. Confirming or denying whether information is held in relation to this part of the request would reveal something about the way cyber attacks are recorded including whether or not certain details about the nature and effects of attacks are held. A confirmation that information is held for example may give an indication to the success or otherwise of an attack. A denial on the other hand may indicate vulnerabilities in the system or that a particular type of attack was unsuccessful. The Commissioner recognises that terrorists and other malicious actors can be highly motivated and may go to great lengths to gather intelligence. Therefore, although seemingly harmless, confirming or denying whether information such as a monthly breakdown of the number of recorded cyber attacks, the nature, and effects of those attacks is held, may assist malicious actors when pieced together with existing or prospectively available information whether gathered lawfully or not.

28. The Commissioner has therefore concluded that MOJ was not entitled to rely on section 31(3) with respect to Part 1 of the request but was entitled to engage same with respect to Part 2 of the request.

Public interest test

29. The Commissioner next considered whether in all the circumstances of the case the public interest in maintaining the exclusion of the duty to confirm or deny outweighs the public interest in disclosing whether it holds information within the scope of Part 2 of the request. Having found that section 31(3) was not engaged with respect to Part 1 of the request, there is no requirement for her to conduct a public interest test.

30. The complainant has correctly pointed out that given the amounts spent by the government on cyber security there is a public interest in knowing how robust the systems in place are. In the Commissioner's

view, confirming or denying whether information is held would only provide limited insight in that regard. However, this limited benefit would clearly be outweighed by the damage such confirmation or denial is ultimately likely to cause to the prevention or detection of crime. The complainant is right to point out that transparency would increase public confidence in government ICT systems and that this would be in the public interest. However, this must be balanced against the stronger public interest in not undermining confidence in government ICT systems by revealing information which would be useful to malicious actors intent on causing criminal damage to the UK and its institutions.

31. Therefore, the Commissioner has concluded that in all the circumstances of the case the public interest in maintaining the exclusion at section 31(3) outweighs the public interest in confirming or denying whether any information is held with respect to Part 2 of the request.

Right of appeal

32. 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@hmcts.gsi.gov.uk
    Website: www.justice.gov.uk/tribunals/general-regulatory-chamber

33. 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.

34. 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 .....

Gerrard Tracey
Principal Adviser
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF