Decision Notice

Decision 084/2016: Mr N and the Chief Constable of Police Scotland

Back-end software and operating system for Centurion

Reference No: 201502011
Decision Date: 12 April 2016

Scottish Information Commissioner

Summary

On 25 May 2015, Mr N asked the Chief Constable of Police Scotland (Police Scotland) for information about the back-end software and operating system on which its Centurion software runs.

Police Scotland withheld the information under sections 35(1)(a) and (b) of FOISA (Law enforcement).

The Commissioner investigated and found that Police was entitled to withhold the requested information under section 35(1)(a) of FOISA.

Relevant statutory provisions

Freedom of Information (Scotland) Act 2002 (FOISA) sections 1(1) and (6) (General entitlement); 2(1)(b) (Effect of exemptions); 35(1)(a) and (b) (Law enforcement)

The full text of each of the statutory provisions cited above is reproduced in Appendix 1 to this decision. The Appendix forms part of this decision.

Background

1. On 25 May 2015, Mr N made a request for information to Police Scotland. He noted that Police Scotland's Counter Corruption Unit uses a software system called Centurion to record cases of complaints and misconduct, and asked if it ran on Oracle, SQL Server or Access as a back-end. He also asked if it ran on Microsoft XP, Vista, 7 or 8 as an operating system.

2. Police Scotland responded on 23 June 2015, withholding the requested information under sections 35(1)(a) and (b) of FOISA. Police Scotland stated that disclosing the information had the potential to compromise its IT structure, and could undermine policing and jeopardise national security. It considered that disclosing the information could make its IT systems vulnerable to hacking.

3. On 24 June 2015, Mr N wrote to Police Scotland requesting a review of their decision on the basis that he did not accept that disclosure of the information would affect national security. He believed that the response from Police Scotland was "incorrect on many levels".

4. Police Scotland notified Mr N of the outcome of their review on 17 July 2015. They upheld their original decision without modification.

5. On 30 October 2015, Mr N applied to the Commissioner for a decision in terms of section 47(1) of FOISA. Mr N stated he was dissatisfied with the outcome of Police Scotland's review because he did not accept that the exemption applied to the withheld information for the reasons given by Police Scotland (which he believed to be technically incorrect). He considered that the security of the IT systems used by Police Scotland was of paramount importance and argued that it would be in the public interest for the information to be disclosed.

Investigation

6. The application was accepted as valid. The Commissioner confirmed that Mr N made a request for information to a Scottish public authority and asked the authority to review its response to that request before applying to her for a decision.

7. On 16 November 2015, Police Scotland were notified in writing that Mr N had made a valid application. Police Scotland were asked to send the Commissioner the information withheld from Mr N. Police Scotland provided the information and the case was allocated to an investigating officer.

8. Section 49(3)(a) of FOISA requires the Commissioner to give public authorities an opportunity to provide comments on an application. Police Scotland were invited to comment on this application (and answer specific questions) including justifying their reliance on any provisions of FOISA they considered applicable to the information requested.

9. Police Scotland responded with submissions in support of their position that the information was properly withheld from Mr N in terms of sections 35(1)(a) and (b) of FOISA.

10. Mr N was invited to provide his views as to why the withheld information should be disclosed, and did so.

11. Police Scotland were asked for further comments as to why disclosure of the withheld information would result in the harm identified in the exemption, and did so.

Commissioner's analysis and findings

12. In coming to a decision on this matter, the Commissioner considered all of the withheld information and the relevant submissions, or parts of submissions, made to her by both Mr N and Police Scotland. She is satisfied that no matter of relevance has been overlooked.

Section 35(1)(a) and (b) of FOISA – Law enforcement

13. Section 35(1)(a) exempts information if its disclosure would, or would be likely to, prejudice substantially the prevention or detection of crime. As the Commissioner's guidance on this exemption[1] highlights, the term "prevention or detection of crime" is wide ranging, encompassing any action taken to anticipate and prevent crime, or to establish the identity and secure prosecution of persons suspected of being responsible for crime. This could mean activities in relation to specific (anticipated) crime or wider strategies for crime reduction and detection.

14. Section 35(1)(b) exempts information if its disclosure would, or would be likely to, prejudice substantially the apprehension or prosecution of offenders. As the Commissioner's guidance also states, there is likely to be a considerable overlap between information relating to "the apprehension or prosecution of offenders" and that relating to "the prevention or detection of crime". She considers that section 35(1)(b) relates to all aspects of the process of identifying, arresting or prosecuting those suspected of being responsible for criminal activity. Again, this term could refer to the apprehension or prosecution of specific offenders or to more general techniques (such as investigative processes and use of police intelligence).

15. There is no definition of "substantial prejudice" in FOISA, but the Commissioner considers the authority would have to identify harm of real and demonstrable significance, which would be likely, at least, to follow disclosure, and more than simply a remote possibility.

[1] http://www.itspublicknowledge.info/Law/FOISA-EIRsGuidance/section35/Section35.aspx

Police Scotland's submissions

16. Police Scotland submitted that disclosure of the information requested by Mr N could increase the vulnerability of their IT systems and infrastructure generally. They explained that they rely on the availability of IT solutions and systems so that police officers and staff are equipped to fulfil their roles. Much of the infrastructure and many of the systems used relate to matters such as support functions, but the vast majority relate to the prevention and detection of crime and the apprehension or prosecution of offenders. Police Scotland considered that if the availability or effectiveness of these systems was compromised in any way, this would significantly prejudice their ability with regard to their law enforcement role.

17. To reduce the possibility of an increased risk of cyber-attack, Police Scotland stated that they consciously release very little detail about their IT infrastructure into the public domain. Their IT experts considered that disclosure of the information would be invaluable to those intent on breaching the IT safeguards currently in place.

18. Police Scotland considered that cyber-attacks are very much an area where every small piece of information, however innocuous it seems, can be added together to form a detailed overview of the infrastructure in place and, crucially, where its vulnerabilities lie and how best to attack it. They made it clear that they were not suggesting that disclosure of the information would lead directly to a cyber-attack which otherwise would not have occurred. However, they were concerned that, armed with additional information about their IT infrastructure, "cyber-attacks could be specifically targeted to take advantage of vulnerabilities in our systems".

19. If individuals were armed with additional knowledge of their IT infrastructure, Police Scotland submitted such attacks were more likely to be successful. They believed that "disclosure of the information sought would serve to increase that risk as it points to a particular vulnerability".

20. Police Scotland considered that any disruption at all to their systems could have potentially catastrophic consequences, which could range from access to sensitive personal data being compromised due to a system being off-line for a period of time. They submitted that they have a statutory duty with regard to the prevention and detection of crime and the apprehension or prosecution of offenders. This role would be prejudiced by disclosure of the information sought as any improvement in the quality of cyber-attack faced by Police Scotland would have a direct impact on the availability of critical systems and/or the diversion of human resources and finances.

21. Police Scotland stated that they have accepted that cyber-attacks or attempted cyber-attacks are inevitable and have dedicated time and financial resources to the prevention of such attacks. However, they took the view that, in a time of budget constraints, not every potential vulnerability could be eliminated and their aim was to make it is as difficult as possible to for individuals to threaten Police Scotland in this way.

Mr N's submissions

22. Mr N commented that Police Scotland's response seemed to indicate that releasing information about the back-end database of a piece of software used by one department of Police Scotland and the operating system it runs on would somehow open up the whole of Police Scotland to being hacked. Mr N considered that the only way a database could be 'hacked' would be if it were on (or connected to) a machine which was exposed to the internet. He suspected that the advice upon which Police Scotland had based its refusal was "political" rather than "technical".

23. However, Mr N expressed concern that Police Scotland would have servers containing sensitive information open to the internet. He argued that if the software was running on an older version of Windows, it was highly vulnerable to being hacked and the information being disclosed to the public.

24. Mr N explained that he would expect successive versions of the software to be more and more secure. As the information held on the Centurion database is sensitive, he would expect this to be addressed. He would expect to see countermeasures to all the different types of attacks which are possible against software, especially databases. He commented that many versions of database languages (such as SQL, MySQL, NoSQL, etc.) are very vulnerable to attacks and he expected the police to maintain and insist upon the highest level of database.

The Commissioner's conclusion

25. The Commissioner is being asked to judge whether disclosure of information about an IT operating system and software is likely to increase the chance that a hacker would learn about a potential weakness and exploit it, which would affect Police Scotland's ability to prevent crime and apprehend offenders. Police Scotland has explained why it believes that disclosure would increase any potential vulnerability to attack. Mr N has acknowledged that if the Centurion database is being run on outmoded software or an insecure operating system, it is "incredibly vulnerable to being hacked".

26. In the circumstances, the Commissioner accepts that disclosure of the requested information would increase the likelihood that a determined individual would seek to disrupt Police Scotland's systems, and, if successful, that this would result in the harm identified by Police Scotland.

27. The Commissioner agrees with Mr N that some of the arguments put forward by Police Scotland appear to be largely hypothetical in nature, such as the claim that disclosure would jeopardise national security. The Commissioner has not been presented with any substantive arguments or evidence to show that national security would be threatened in any immediate sense, if the information covered by Mr N's request was disclosed. However, she accepts that disclosure of the information has the potential to increase risk of a successful hacking attack, which would (at the least) be disruptive to Police Scotland.

28. The Commissioner is mindful of the fact that disclosure under FOISA is in effect disclosure into the public domain, not just to an individual. Mr N may have the best motives for seeking this information, in seeking to highlight the need for Police Scotland to operate in a secure IT environment, but he is not the only person who would have access to the information if it was disclosed in response to the request.

29. Having considered the submissions from Mr N and Police Scotland, the Commissioner is satisfied that disclosing the details of the back-end software and operating system used would, or would be likely to, prejudice substantially "the prevention or detection of crime". The Commissioner is satisfied that disclosure would disrupt the systems used by Police Scotland to complete such work in detecting or preventing crime. Consequently, she is satisfied that this information falls within the scope of the exemption in section 35(1)(a) of FOISA.

30. In relation to the exemption in section 35(1)(b) of FOISA, Police Scotland have not provided any detailed reasons to show why disclosure of the requested information would prejudice substantially the "apprehension or prosecution of offenders". Police Scotland's submissions

have focussed on the disruption that disclosure would cause to its IT systems, but have not explained how such disruption would impact upon the actual apprehension or prosecution of offenders. Therefore the Commissioner has concluded that the exemption in section 35(1)(b) of FOISA was wrongly applied to the withheld information.

The public interest test

31. As the Commissioner has found that the exemption in section 35(1)(a) was correctly applied to the withheld information, she is required to consider the public interest test in section 2(1)(b) of FOISA. She has therefore considered whether, in all the circumstances of the case, the public interest in disclosing the withheld information is outweighed by the public interest in maintaining the exemption in section 35(1)(a) of FOISA.

Police Scotland's submissions

32. Police Scotland considered that there were factors that would favour the disclosure of the withheld information in the public interest. As a public authority, they are accountable for the management of their finances and the decisions made with regard to distribution of their budget, including the proportion dedicated to particular elements of Policing. They submitted that disclosure of the information would inform the public to an extent as to the investment in this area and the IT infrastructure in place within Police Scotland.

33. On balance, however, Police Scotland considered that factors favouring non-disclosure were stronger. It would not be in the public interest for information to be disclosed which might increase the risk of a successful cyber-attack, leaving Police Scotland unable to properly fulfil its functions with regard to the prevention and detection of crime. Police Scotland argued that this would inevitably lead to a significant increase in the risk to public safety. Any successful cyber-attack would also inevitably lead to a significant increase in costs.

Mr Ns submissions

34. Mr N argued that full disclosure would be in the public interest and it would ensure that, if potential vulnerabilities exist, they will be addressed.

35. Mr N explained that he would like to start with an assessment of the information and cyber security of these secret databases, especially as he suspects that the database is administered differently to, for example, the Police National Computer. Mr N strongly suspects Police Scotland are administering this database locally, i.e. on their own systems, and as such, expects that it will be poorly protected. Given that the database holds sensitive information, he was concerned about the consequences, if the security of the database was breached. If he received information confirming his suspicions, he intended to lobby Police Scotland to apply the necessary protections to the database.

The Commissioner's conclusions

36. The Commissioner acknowledges the general public interest in transparency and accountability. She accepts that disclosure of the information would allow public scrutiny of the level of software used by Police Scotland and allow an assessment of whether the Centurion database is secure.

37. On the other hand, the Commissioner has already acknowledged that disclosure of the information would, or would be likely to, lead to substantial prejudice for the purposes of section 35(1)(a) of FOISA. This would not be in the public interest.

38. Having balanced the public interest for and against disclosure, the Commissioner has concluded that the arguments against disclosure should prevail in this particular case.

Consequently, she is satisfied that, in all the circumstances of the case, the public interest in maintaining the exemption in section 35(1)(a) outweighs that in disclosure of the information under consideration.

39. The Commissioner therefore finds that Police Scotland were entitled to withhold the information under the exemptions in section 35(1)(a) of FOISA.

Decision

The Commissioner finds that the Chief Constable of the Police Service of Scotland complied with Part 1 of the Freedom of Information (Scotland) Act 2002 in responding to the information request made by Mr N.

Appeal

Should either Mr N or Police Scotland wish to appeal against this decision, they have the right to appeal to the Court of Session on a point of law only. Any such appeal must be made within 42 days after the date of intimation of this decision.

Margaret Keyse
Head of Enforcement

12 April 2016

Appendix 1: Relevant statutory provisions

Freedom of Information (Scotland) Act 2002

1 General entitlement

(1) A person who requests information from a Scottish public authority which holds it is entitled to be given it by the authority.

…

(6) This section is subject to sections 2, 9, 12 and 14.

2 Effect of exemptions

(1) To information which is exempt information by virtue of any provision of Part 2, section 1 applies only to the extent that –

…

(b) in all the circumstances of the case, the public interest in disclosing the information is not outweighed by that in maintaining the exemption.

…

35 Law enforcement

(1) Information is exempt information if its disclosure under this Act would, or would be likely to, prejudice substantially-

(a) the prevention or detection of crime;

(b) the apprehension or prosecution of offenders;

…

Scottish Information Commissioner
Kinburn Castle
Doubledykes Road
St Andrews, Fife
KY16 9DS

t 01334 464610
f 01334 464611
enquiries@itspublicknowledge.info

www.itspublicknowledge.info