



Scottish Information
Commissioner
www.foi.scot

Decision Notice 076/2025

Operating systems of computers

Authority: NHS Tayside

Case Ref: 202401559

Summary

The Applicant asked the Authority for the numbers of computers using specified operating systems. The Authority withheld the information on the grounds that disclosure would, or would be likely to, prejudice substantially the prevention or detection of crime. The Commissioner investigated and found that the Authority had correctly withheld the information.

Relevant statutory provisions

Freedom of Information (Scotland) Act 2002 (FOISA) sections 1(1), (2) and (6) (General entitlement); 2(1)(b) (Effect of exemptions); 16(1) and (2) (Refusal of request); 35(1)(a) (Law enforcement); 47(1) and (2) (Application for decision by Commissioner)

Background

1. On 5 November 2024, the Applicant made a request for information to the Authority. He asked for the number of computers used by the Authority with the following operating systems installed:
 - Windows 95
 - Windows 98
 - Windows XP
 - Windows 7

- Windows 8 or Windows 8.1
 - Windows 10
2. The Authority responded on 6 November 2024. It notified the Applicant that it could not answer their questions as it considered the information to be exempt under section 31 (National Security and Defence) of FOISA. The Authority explained that disclosure would increase the risk of a cyber-attack, which was a criminal offence and, in these circumstances, the public interest favoured withholding the information.
 3. Later that same day, on 6 November 2024, the Applicant wrote to the Authority requesting a review of its decision. The Applicant did not consider that section 31 of FOISA was relevant to the information being withheld and he argued that the Authority was not entitled to withhold it. The Applicant also disagreed with the Authority's consideration of the public interest test.
 4. The Authority notified the Applicant of the outcome of its review on 21 November 2024. The Authority conceded that it had initially applied the wrong exemption and it explained that it was withholding the information under section 35 of FOISA. The Authority reaffirmed its view that the public interest lay in withholding the information. The Applicant wrote to the Authority the same day and asked it to confirm which part of section 35 it was seeking to apply. The Authority responded later that day and clarified that it was withholding the information under section 35(1)(a) of FOISA.
 5. On 27 November 2024, the Applicant wrote to the Commissioner, applying for a decision in terms of section 47(1) of FOISA. The Applicant stated that he was dissatisfied with the outcome of the Authority's review because it had not provided sufficient justification under FOI to withhold the information. The Applicant argued that the exemption did not apply, and the public interest had not been properly considered.

Investigation

6. The Commissioner determined that the application complied with section 47(2) of FOISA and that he had the power to carry out an investigation.
7. On 3 December 2024, the Authority was notified in writing that the Applicant had made a valid application. The Authority was asked to send the Commissioner the information withheld from the Applicant. The Authority 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. The Authority was invited to comment on this application and to answer specific questions. These related to its reasons for applying section 35(1)(a) of FOISA and to ask for details of how the Authority assessed the public interest.

Commissioner's analysis and findings

9. The Commissioner has considered all of the submissions made to him by the Applicant and the Authority.

The withheld information

10. The withheld information is one email from the Authority's Digital Directorate which states the list of operating systems given in the request against the number of computers within the Authority using each of those systems. The number of computers using each operating system ranges from zero to approximately 15,000.

Section 35(1)(a) – Law enforcement (prevention or detection of crime)

11. The Authority submitted that all of the information captured by the request was exempt from disclosure by virtue of the exemption in section 35(1)(a) of FOISA.
12. Under section 35(1)(a) of FOISA, information is exempt information if its disclosure would, or would be likely to, prejudice substantially the prevention or detection of crime. As the Commissioner's [briefing on section 35](#)¹ notes, the term "prevention or detection of crime" is wide ranging. It encompasses actions taken to anticipate and prevent crime, or to establish the identity and secure prosecution, of people suspected of being responsible for committing a crime. This could mean activities in relation to a specific (anticipated) crime or wider strategies for crime reduction and detection.
13. The exemption in section 35(1)(a) can only apply where disclosure of the information in question would, or would be likely to, prejudice substantially the prevention or detection of crime. FOISA does not define "substantial prejudice", but the Commissioner considers an authority would have to identify harm of real and demonstrable significance. The harm would also have to be at least likely and, therefore, more than a remote possibility. The Authority must be able to demonstrate that some causal relationship exists between the potential disclosure of the information being withheld and the prejudice the exemption is designed to protect against.
14. This exemption is subject to the public interest test in section 2(1)(b) of FOISA.

The Applicant's comments on the exemption

15. The Applicant argued that section 35(1)(a) did not apply to every piece of information that, if released, could minutely increase the probability of a hypothetical situation in which a crime was committed. He cited the Commissioner's briefing on section 35 and noted that the exemption only applied to information that was likely to substantially prejudice the prevention or detection of crime and that there must be real and demonstrably significant damage caused by disclosing the information. The Applicant considered the risk to the Authority in this case, was only a hypothetical possibility.
16. The Applicant argued that revealing the number of computers on which various operating systems are installed did not in itself reveal anything about the details of what is stored on the computers, what networks they are connected to, or how they are used, all of which are necessary in order to "map technologies for weaknesses". He submitted that it was unclear why the Authority took the position that disclosing the information would substantially prejudice the prevention of crime.
17. The Applicant commented that it was relevant that other, similar, authorities had disclosed information in response to similar requests.

¹ <https://www.foi.scot/sites/default/files/2022-04/BriefingSection35LawEnforcement.pdf>

The Authority's comments on the exemption

18. The Authority submitted that section 35(1)(a) was engaged because disclosing what computer operating systems it does or does not currently use would, or would be likely to, give cyber criminals insight into the infrastructure, hardware, software systems, and potential vulnerabilities which may exist within the Authority's estate. If this occurred, the Authority argued that it would likely result in damage to its IT infrastructure and systems.
19. The Authority submitted that, because disclosure under FOISA is disclosure to the wider public domain and that it had no control over what the data is to be used for, it considered that withholding this information in its entirety was appropriate. The Authority explained that it had withheld all of the information in order to avoid releasing any evidence into the public domain that related to its cyber posture/position.
20. The Authority was asked to comment on similar information that had been disclosed by other public authorities. The Authority noted that such disclosures were made some years ago, prior to the withdrawal of support from Microsoft for certain operating systems and, as such, disclosure of the information would have carried much less risk.

The Commissioner's view on the exemption

21. The Commissioner has considered carefully all of the Applicant's and Authority's submissions, as well as the information withheld under the exemption.
22. The Commissioner notes that all of the operating systems mentioned in the Applicant's request are Microsoft operating systems. Microsoft makes [regular announcements](#)² regarding its older operating systems and publicises the dates when support for these systems will be withdrawn. It is well known that operating systems are vulnerable to cyber-attack once Microsoft ceases to provide security updates and support for these products.
23. The request asks for the number of computers, each using a specific operating system from a list of a wide range of Microsoft operating systems, including those which are no longer supported, in addition to some of those which are continually supported and updated. Given this, the Commissioner is satisfied that, even if the number of those computers using unsupported systems is zero, the disclosure of such information into the wider public domain is a substantial risk to the Authority.
24. The Commissioner notes that in recent years there has been a steady trend of cyber enabled and cyber dependant crime increasing in Scotland and the wider UK. He is satisfied that disclosure of the Authority's cyber position into the public domain could be used by malicious actors to the substantial prejudice of the Authority.
25. Given this, the Commissioner accepts that the section 35(1)(a) of FOISA is engaged. He will now go on to consider the public interest test in section 2(1)(b) in relation to the withheld information.

Public interest test

26. The Applicant was dissatisfied with the Authority's assessment of the public interest. He submitted that the Authority's review had not identified or set out the competing arguments as to why the public interest would be served by disclosing, or withholding, the requested information and that no balancing exercise had been carried out.

² <https://learn.microsoft.com/en-us/lifecycle/>

27. The Applicant argued that the Authority had not undertaken sufficient assessment of the content of his request, or considered the specific risks of disclosure of this specific information, or presented its arguments for releasing the information in the public interest.
28. The Authority recognised that disclosure of the information would highlight any ongoing use of older, unsupported legacy systems and the possible risks associated with that. The Authority acknowledged that this would aid transparency and accountability.
29. However, the Authority counter-argued that withholding all of the information protected its systems from attack by cyber criminals and it noted that such threats are widely documented on the internet. The Authority submitted that non-disclosure gave no indication to potential hackers of what operating systems it was using, which limited the hackers capacity to cause substantial harm, which would not be in the public interest.
30. The Authority submitted that it had legal obligations to keep personal information secure and to take appropriate measures to keep information confidential where necessary. The Authority argued that it was not in the public interest to risk the substantial costs it would incur in trying to recover from a cyber-attack, including any regulatory fines that it would be subject to. It explained that, because of the nature of its functions, it had a large amount of personal data, including a lot of very sensitive data – for example, about care and treatment provided to its patients, or casework for child protection reports, and it submitted that it must take all necessary steps to make sure this data was kept safe.
31. The Authority considered there was a greater public interest in protecting personal data held by it, preventing any threat to the integrity of patients' data and avoiding disruption to the services and functions it delivers. On balance, the Authority submitted that the public interest lay in upholding the exemption and withholding information about all of its operating systems.

The Commissioner's view on the public interest

32. The Commissioner has considered the submissions from the Applicant and has examined the Authority's review outcome. The Commissioner agrees with the Applicant that the Authority has not set out the competing arguments in the refusal notice. The Commissioner's [briefing on the public interest](#)³ is clear on this. Authorities must set out the competing public interest arguments and explain why they have concluded that the public interest lies in maintaining the exemption as opposed to releasing the information. For this reason, the Commissioner must find that the Authority failed to issue proper notice under section 16(1) and (2) of FOISA.
33. Notwithstanding, the Authority has laid out the competing arguments in its submissions to the Commissioner (and repeated in this decision), and he has considered these carefully. The Commissioner notes that while the Applicant expressed dissatisfaction with the Authority's consideration of the public interest test, he did not provide any detailed arguments explaining why the public interest favoured disclosure of the information.
34. The Commissioner acknowledges the general public interest in transparency and accountability. He accepts that disclosure of such information would allow public scrutiny of the computer operating systems used by the Authority and allow some assessment of whether those systems are secure and effective.

³ https://www.foi.scot/sites/default/files/2023-07/PublicInterestTestFOISA_2023.pdf

35. However, given the nature and sensitivity of the functions carried out by the Authority and of the wider information held in its IT systems, the Commissioner accepts that there is a very strong public interest in maintaining the integrity and security of those systems and, wherever possible, minimising the risk of cyber-attack.
36. On balance, the Commissioner is satisfied that, in relation to this set of information, the public interest in maintaining the exemption in section 35(1)(a) would outweigh any public interest in disclosure of the information. The Commissioner recognises the vital importance of allowing the Authority to fulfil its functions by maintaining a secure and effective IT environment.
37. The Commissioner is therefore satisfied that the Authority was entitled to withhold the information on the basis that the information was exempt information under section 35(1)(a) of FOISA.

Decision

The Commissioner finds that the Authority partially complied with Part 1 of the Freedom of Information (Scotland) Act 2002 (FOISA) in responding to the information request made by the Applicant.

The Commissioner finds that by correctly withholding information under section 35(1)(a) of FOISA, the Authority complied with Part 1.

However, in failing to set out the competing arguments of the public interest test and thereby failing to issue a proper refusal notice, the Commissioner finds that the Authority failed to comply with section 16(1) and (2) of FOISA.

Given that the Authority's public interest arguments were given to the Commissioner and have been detailed in this decision, the Commissioner does not require the Authority to take any action in respect of this failure.

Appeal

Should either the Applicant or the Authority 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.

Euan McCulloch
Head of Enforcement

25 March 2025