Freedom of Information Act 2000 (FOIA)

Decision notice

Date: 22 February 2017

Public Authority: Network Rail
Address: The Quadrant
Elder Gate
Milton Keynes
MK9 1EN

Decision (including any steps ordered)

1. The complainant has requested information on CCTV and surveillance techniques employed at Edinburgh Waverley train station. Network Rail provided some information as requested but refused to confirm the number of CCTV cameras at the station on the basis of sections 24(1), 31(1)(a) and (b) and 38(1) as well as refusing to confirm or deny if information was held for three other parts of the request by virtue of the exclusions at section 24(2), 31(3) and 38(2) of the FOIA.

2. The Commissioner's decision is that Network Rail has correctly applied section 24(1) to part 1 of the request and section 24(2) to parts 5, 6a and 7 and the public interest in both cases favours maintaining the exemption. She requires no steps to be taken.

Request and response

3. On 15 February 2016, the complainant wrote to Network Rail and requested information in the following terms:

1) How many CCTV surveillance cameras are there in Edinburgh Waverley Station?

2) How much has been spent on installing these cameras in each of the last five years?

3) Please confirm where they are monitored and the body responsible for monitoring and maintaining them?

4) For each of the last five years, please confirm how much funding has been received from third-party organisations to support the costs of installing, maintaining and monitoring CCTV cameras in Edinburgh Waverley Station. Please name the third-party bodies providing funding.

5) Please confirm whether Network Rail uses any visual analytics, such as facial recognition, "gait analysis", or automatic number plate recognition software, in conjunction with the CCTV cameras in Edinburgh Waverley?

6a) If any visual analytics software is in use, please confirm which firm supplies it, how long it has been in use, and please supply any privacy assessment which has been undertaken by Network Rail that relates to the use of the software.

6b) Please confirm how many times a third party body, such as Police Scotland, has partially or wholly taken over the operation of the CCTV cameras in Waverley station in each of the last three calendar years? Please supply the Memorandum of Understanding or other documents that set-out the process for allowing third party bodies to control the CCTV system in Waverley Station.

7) Are there any audio recorders in the station, or sensors with the ability to capture audio from the station? If so, how many of these sensors are installed?

4. Network Rail responded on 14 April 2016. It stated that some information was held but where information was held it was exempt under sections 31(1)(a), (b) and (c) of the FOIA as disclosure would, or would be likely to prejudice the prevention or detection of crime, the apprehension or prosecution of offenders, and/or the administration of justice.

5. Following an internal review Network Rail wrote to the complainant on 9 June 2016. It acknowledged that it had not specifically stated what information was held and Network Rail then explained that information was held for parts 1 and 3 but was being withheld under sections 31(1), no information was held for part 4 and for parts 2, 5, 6a, 6b and 7 Network Rail refused to confirm or deny if information was held by virtue of the exclusion at section 31(3) of the FOIA.

Scope of the case

6. The complainant contacted the Commissioner on 9 June 2016 to complain about the way his request for information had been handled.

7. During the course of the Commissioner's investigation, further discussions occurred between Network Rail and the complainant. As a result of this, Network Rail provided an estimate of the total amount spent on installing CCTV in response to part 2, provided information in relation to part 3 and answered part 6b.

8. For the remaining questions, Network Rail amended its position in some cases and withdrew its reliance on subsection 31(1)(c) in relation to part 1 whilst still maintaining its reliance on subsection (a) and (b). For parts 5, 6a and 7 Network Rail clarified that it still would not confirm or deny if information was held by virtue of the exclusion at 31(3) of the FOIA and that the subsections that would be likely to be prejudiced if it confirmed or denied if information was held were subsections 1(a) and (b).

9. In addition to this, Network Rail introduced the section 24 and 38 exemptions which had prior to this not been specifically referenced, albeit mentions of national security and public safety had been contained in its responses. Network Rail stated that as well as section 31(3) it also considered sections 24(2) and 38(2) provided an exclusion from either confirming or denying if information was held for parts 5, 6a and 7. Section 24(1) and 38(1) were also cited to withhold the information held for part 1 of the request.

10. The Commissioner therefore considers the scope of her investigation to be to establish if Network Rail has correctly withheld or refused to confirm or deny if information is held for parts 1, 5, 6a and 7. The relevant exemptions are as follows:

    - Part 1 – section 31(1)(a) and (b), 24(1) and 38(1)
    - Parts 5, 6a and 7 – sections 31(3), 24(2) and 38(2).

Reasons for decision

Section 24(1) - National security

11. Section 24(1) states that:

    'Information which does not fall within section 23(1) is exempt information if exemption from section 1(1)(b) is required for the purpose of safeguarding national security'.

12. The FOIA does not define the term national security. However in *Norman Baker v the Information Commissioner and the Cabinet Office*[1] the Information Tribunal was guided by a House of Lords case, *Secretary of State for the Home Department v Rehman* [2001] UKHL 47, concerning whether the risk posed by a foreign national provided grounds for his deportation. The Information Tribunal summarised the Lords' observations as follows:

    - "national security" means the security of the United Kingdom and its people;
    - the interests of national security are not limited to actions by an individual which are targeted at the UK, its system of government or its people;
    - the protection of democracy and the legal and constitutional systems of the state are part of national security as well as military defence;
    - action against a foreign state may be capable indirectly of affecting the security of the UK ; and
    - reciprocal co-operation between the UK and other states in combating international terrorism is capable of promoting the United Kingdom's national security.

13. Furthermore, in this context the Commissioner interprets 'required for the purposes of' to mean reasonably necessary. Although there has to be a real possibility that the disclosure of requested information would undermine national security, the impact does not need to be direct or immediate.

14. The Commissioner has gone on to consider this in the context of part 1 of the request where the section 24(1) exemption has been cited as a basis for withholding information. Part 1 asked how many CCTV cameras there are at Edinburgh Waverley train station.

15. Network Rail considers there is a close relationship between the sections 24, 31 and 38 exemptions but as the section 24 exemption concerns national security this is the first exemption to be considered by the Commissioner in this case.

[1] (EA/2006/0045)

16. Network Rail believes that disclosing information about security arrangements at a major transport hub would assist in the planning of a terrorist attack and this would increase the risk to national security. Disclosing the number of cameras at the station would place information into the public domain and can then be combined with other information to provide intelligence to those wishing to target a transport hub.

17. To support its position, Network Rail has explained the significance of Edinburgh Waverley station as a key transport hub, being Britain's largest train station outside of London. CCTV in the station is used for a wide variety of uses including deterring and preventing crime and terrorist activities, detecting crime and terrorist activities, assisting the emergency services and providing evidence in criminal proceedings.

18. Network Rail argues that rail stations have been recognised as targets for terrorism due to the potential for mass casualties and wider disruption. The British Transport Police (BTP) was established as a specialist police force for the railway and they work in partnership with Network Rail and other rail operators to provide efficient and effective railway policing. In written evidence to the Scottish Government Public Audit Committee in 2015, the BTP explained the threat to the rail network:

    "The threat level to Britain's railways is Severe, meaning an attack is highly likely, and attacks on public transport systems generally have long been seen as a priority and attractive to terrorists. Since 1970, for example, there have been more than 4,000 recorded attacks targeting public transport worldwide. Of which, those involving bombs placed on trains or on buses account for the largest (and most lethal) proportion (35%)."[2]

19. The current threat level in the UK is severe and has remained at this level for some time. In addition to this, there have been attacks at transport hubs since the request was made, most notably at Brussels airport and Maalbeek metro station in central Brussels.

20. The Commissioner accepts that the above arguments demonstrate that rail stations are likely targets for terrorist attacks but she must now consider whether disclosing details of the CCTV cameras in operation at Waverley station would be likely to increase the risk of such an attack.

---

2 https://www.btp.police.uk/pdf/BTP%20Public%20Audit%20Committee%20Evidence%20Submission1.pdf

21. In arguing this point, Network Rail has highlighted that a joint initiative between the Department for Transport (Dft), the BTP and the rail industry was launched with the aim of building a more vigilant network. As part of this the BTP asked the public to be vigilant and report anything unusual including anyone checking out security arrangements such as CCTV cameras.

22. Network Rail considers the withheld information – the number of CCTV cameras in the station – concerns the techniques and methodologies for policing the rail network. Revealing the number of cameras would provide information on the security capabilities of Network Rail, showing the strength or weakness of the security at the station.

23. Network Rail further argues that if the information becomes available and accessible, usually via the internet, it can be used in the planning of an attack. The collection of 'open source' material to compile profiles and identify targets is a recognised strategy employed by those planning terrorist activities and the Commissioner has previously accepted this. For example in a case[3] relating to the amount spent by a particular police unit the Commissioner founds that the information *"may in itself seems insignificant, when it connected with other open source material it could allow quite effective profiling of potential targets and comparison of their respective vulnerabilities, whether by a terrorist, criminal or fixated person … publicly available information both on the internet and elsewhere remains a powerful source of intelligence for those intending to target the security of the UK."*

24. The Commissioner still has some concerns as to whether disclosing the number of cameras at the station, even taking into account the comments in the above paragraph, would assist in the planning of an attack other than allowing for comparison of the number of cameras at other stations (should this information be publicly available). Even then, it is reasonable that different stations will have different numbers of CCTV cameras and this will not necessarily be down to the risk of an attack at that station but could also be due to other factors such as size, footfall, and number of trains passing through and/or stopping.

25. Network Rail has provided some further arguments on this point. As Edinburgh Waverley is a listed building a detailed public planning process took place to ensure appropriate modifications were applied when the CCTV cameras were installed. This provides a benchmark of CCTV camera coverage at a specific point in time following the 2005

[3] FS50368290

attacks on the London Underground and the 2007 attack on Glasgow Airport, including the number and locations of cameras. In addition to this, detailed plans of the station are also publicly available, therefore if the information at part 1 of the request were to be disclosed this could be combined with information, including detailed plans of the station and the locations of some of the CCTV cameras within the station from an earlier point in time. This could allow for more accurate mapping of the CCTV camera locations in the station.

26. The Commissioner has also considered whether the number of cameras is already available should a motivated individual choose to find it out. Of course, it is possible that such an individual could visit the station and physically count and map the cameras in areas accessible to the public. Network Rail argues this is not the same as a public authority officially confirming the number via a public disclosure and points to the Commissioner's decision[4] on a case relating to the locations of fire hydrants in which she found that *"disclosure of a collated list of the precise location of every hydrant in the WMFS area would disclose into the public domain additional information than is available through hydrants being visible."*

27. In addition to this is the concept of 'hostile reconnaissance' – the idea that a terrorist will physically attend a location for the purpose of gaining the necessary intelligence to support an attack on a site. In another decision considered by the Information Tribunal[5] it was accepted that the public disclosure of information reduced the opportunity for intervention. It was acknowledged that suspicious behaviour is more likely to be detected and apprehended if an individual cannot access information about security arrangements via the internet and instead has to physically visit a site in order to view and assess the security arrangements.

28. The Commissioner does recognise that the number of CCTV cameras in a station does not in itself seem to be information which would increase the likelihood of a terrorist attack should it be disclosed. However, Network Rail has provided convincing arguments supported by evidence from a number of sources that show the CCTV network and the way this operates is an integral part of rail stations protecting against terrorist attacks. The Commissioner particularly puts weight to the argument that if a motivated individual had to physically attend a rail station to map

[4] FS50585724

[5] EA/2012/0127

the locations and numbers of CCTV cameras this may arouse suspicion and lead to the detection and apprehension of the individual, therefore disclosing the number of cameras reduces the opportunity to detect suspicious behaviour. In addition to this, the situation at Edinburgh Waverley is different from that at other stations, and there are already detailed plans of the station in the public domain. The Commissioner cannot discount the 'mosaic' argument that disclosing the number of CCTV cameras now and using this with information already in the public domain could lead to an individual obtaining a very detailed view of the surveillance and security arrangements in operation at the station.

29. For this reason the Commissioner accepts there is a link between the requested information – the number of CCTV cameras at Edinburgh Waverley station – and the increased likelihood of a terrorist attack and therefore the risk to national security. The Commissioner therefore considers the section 24(1) exemption is engaged in relation to the information held for part 1 of the request.

Public interest arguments in favour of disclosure

30. The complainant argues there are concerns about the use and regulation of CCTV and other technologies that have been raised in the Scottish Parliament and at Westminster. He argues that disclosing the information would not benefit those wanting to engage in terrorist activities and there is a public interest in openness and transparency in controversial technologies.

31. The complainant also draws attention to the Surveillance Camera Code of Practice[6] which states that there must be as much transparency in the use of a surveillance camera system as possible.

32. Network Rail recognises the public interest in being open and accountable for its operations and accepts that disclosing information in this case would help to inform public debate and ease public concerns about the use of surveillance technology and CCTV in public spaces. Network Rail argues much of the public interest in accountability has been met by the disclosure of information in relation to several parts of the request.

Public interest arguments in favour of maintaining the exemption

---

6 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf

33. Balanced against the public interest in transparency and accountability, Network Rail argue that disclosing the requested information would provide those interested in committing acts of terrorism with factual information to increase their confidence and make an attack more likely which would not be in the public interest.

34. Network Rail points to the public interest arguments being linked to the arguments already presented as to how disclosure would impact on the safeguarding of national security. That is that the information concerns security arrangements at a major transport hub at a time when the threat level for international terrorism is severe and there is a clear public interest in maintaining security at the station and in avoiding prejudice to BTP's ability to detect suspicious behaviour.

Balance of the public interest arguments

35. In the Commissioner's opinion there is an obvious and weighty public interest in the safeguarding national security. In the particular circumstances of this case the Commissioner agrees with Network Rail that it would be firmly against the public interest to undermine security at a major UK transport hub given the current threat level. She considers Network Rail have clearly argued how putting this information in the public domain could lead to an increased risk of an attack and why this would not be in the public interest.

36. Nevertheless, the Commissioner recognises that section 24 is not an absolute exemption and therefore there may be circumstances where the public interest favours disclosure of information which engages this exemption. Whilst CCTV and surveillance is an issue which is of concern to the public, particularly with regard to the impact of increased surveillance on individuals privacy, and therefore disclosing information which informs public debate of these issues would be of some public interest; the Commissioner does not consider that this argument carries sufficient weight to override the significant and weighty public interest in ensuring the security of rail network and the UK's transport hubs.

37. The Commissioner has therefore concluded that the public interest favours maintaining the exemption contained at section 24(1) of FOIA in relation to the information held for part 1 of the request.

Section 24(2)

38. For the remaining requested information (parts 5, 6a and 7) Network Rail relies on the exclusion at section 24(2) from the requirement to either confirm or deny if the information is held as to do so would in itself impact on the safeguarding of national security (section 24(1)).

39. For part 5 the information requested is whether or not Network Rail uses visual analytics or automatic number plate recognition software in conjunction with CCTV cameras; for part 6a the information requested is who supplied the visual analytics software (if used) and details of any privacy impact assessment undertaken; and for part 7 the information requested is whether or not there are audio recorders in station.

40. Network Rail has argued that confirming or denying if it held information for any of the above parts of the request would place information into the public domain where it can be widely accessed and combined with other public information to provide intelligence to terrorists or those with ill-intent who may want to target a major transport hub.

41. Network Rail considers the arguments are the same as for the information held for part 1 but in this case believes that either confirming or denying if the information is held would have the prejudicial effect argued for part 1 of the request where it was confirmed the information was held. This is because parts 5, 6a and 7 seek information about the security arrangements at Waverley station and focus on specific capabilities of the CCTV system such as whether specific techniques are in use at the station. Confirming or denying whether or not these more advanced surveillance techniques are undertaken at the station would in itself reveal information which could facilitate an attack either by informing an assessment of possible strengths or by highlighting vulnerabilities. This information would be of value in assisting those with intent on making an informed assessment of the likelihood of carrying out a successful attack at the site.

42. The Commissioner accepts that a 'neither confirm nor deny' response is appropriate in this case. For the same reasons as she accepted the section 24(1) exemption was engaged in relation to the information held for part 1 of the request, she accepts that confirming or denying if the other information is held could increase the likelihood of an attack. The Commissioner does not intend to revisit the same arguments again as she has already analysed them earlier in this decision notice but does want to add that the remaining information requested relates to more advanced techniques that may or may not be used in the station. With part 1 of the request it is quite clear that the station operates CCTV cameras so confirming this is not disclosing information not already known, however it is not known whether Network Rail employs visual analytics or audio recording. Therefore confirming or denying if it holds information will reveal something, whether this is the use of these techniques or the absence of them, which is not already publicly known.

43. This information, for the same reasons as disclosing the number of CCTV cameras, if it were to be disclosed would increase the risk of an attack

and therefore the Commissioner finds that the exclusion from the duty to confirm or deny at section 24(2) has been correctly applied.

44. The Commissioner must still consider the public interest arguments and again does not wish to repeat those already set out in this notice, all of which are also applicable to parts 5, 6a and 7 of the request. In addition the Commissioner places particular emphasis on the public interest in neither confirming nor denying if this information is held as to do so would reveal information about advanced techniques and potentially reveal weaknesses that can be targeted or show areas of strength that need to be circumvented. Currently any motivated individual would be unaware of what surveillance techniques are in use and providing any additional information on this will be of interest to those with ill-intent in informing whether to carry out an attack. This is a clear and substantive argument in favour of not confirming or denying if the information is held.

45. The Commissioner therefore finds that Network Rail correctly relied on the exclusion at section 24(2) to neither confirm nor deny it held the information requested at parts 5, 6a and 7 and the public interest favours maintaining the exemption.

Right of appeal

46. 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

47. 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.

48. 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 ……

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