Freedom of Information Act 2000 (Section 50)

Decision Notice

Date: 3 March 2011

Public Authority: **The Metropolitan Police Service**
Address: **20th Floor Empress State Building**
Lillie Road
London SW6 1TR

Summary

The complainant requested information from the Metropolitan Police Service (MPS) about people convicted under the refusal to decrypt legislation. The MPS ultimately confirmed it held information within the scope of the request but withheld it citing the exemptions in sections 40(2) (personal information) and 30(1) (investigations and proceedings). It also neither confirmed nor denied that it held any other relevant information citing the exemptions in sections 23(5) (information supplied by or relating to bodies dealing with security matters) and 24(2) (national security). The Commissioner focussed his investigation on the personal information exemption. He found that the exemption at section 40(2) is engaged and requires no steps to be taken. However, the Commissioner identified a series of procedural shortcomings on the part of the public authority relating to delay (section 10) and failure to explain application of exemptions (section 17).

The Commissioner's Role

1. The Commissioner's duty is to decide whether a request for information made to a public authority has been dealt with in accordance with the requirements of Part 1 of the Freedom of Information Act 2000 (the "Act"). This Notice sets out his decision.

Background

2. Encryption is a form of security that turns information, images, programs or other data into an unreadable coded message by applying a set of complex algorithms to the original material. These algorithms transfer the data into streams or blocks of seemingly random

alphanumeric characters. An encryption key might encrypt, decrypt, or perform both functions, depending on the type of encryption software being used.

3. On 24 November 2009 an article was published in *The Register* about an individual, identified only by the initials JFL, who was sentenced under Part III of the Regulation of Investigatory Powers Act (RIPA). The article stated:

> *"his crime was a persistent refusal to give counter-terrorism police the keys to decrypt his computer files."*

4. RIPA regulates the powers of public bodies to carry out surveillance and investigation, and covers the interception of communications. It was introduced to take account of technological change such as the growth of the internet and strong encryption.

5. RIPA regulates the manner in which certain public bodies may conduct surveillance and access a person's electronic communications. For example, it enables certain public bodies to demand that someone hands over cryptographic keys to encrypted digital data.

6. RIPA can be invoked by government officials specified in the Act on the grounds of national security, and for the purposes of detecting crime, preventing disorder, public safety, protecting public health, or in the interests of the economic well-being of the United Kingdom.

The Request

7. The complainant wrote to the Metropolitan Police Service (MPS) on 24 November 2009 with the following request:

> *"Please let me have all information relating to people convicted under the refusal to decrypt legislation, like mentioned in http://www.theregister.co.uk/2009/11/24/ripa_jfl/."*

8. The MPS responded on 12 February 2010. The MPS neither confirmed nor denied that it held the requested information, citing the exemptions in sections 40(5) (personal information), 23(5) (information supplied by, or relating to, bodies dealing with security matters), 24(2) (national security), 30(3) (investigations and proceedings), 31(3) (law enforcement) and 38(2) (health and safety).

9. The complainant requested an internal review on 19 May 2010.

10. The MPS varied its decision in its internal review correspondence which it provided to the complainant on 30 June 2010. It confirmed it held

information in relation to one specific conviction in relation to the offence of *"Fail to disclose key to protected information",* and disclosed some information about the conviction to the complainant.

11. However, it continued to withhold other information about the conviction and within the scope of his request citing the exemption in section 40(2). Further, it neither confirmed nor denied that it held any further information within the scope of the request, citing the exemptions in sections 23(5) and 24(2). No reference was made to sections 31 or 38.

The Investigation

Scope of the case

12. The complainant contacted the Commissioner on 21 June 2010 to complain about the way his request for information was being handled. At that stage his complaint was that he had not received a response from the Metropolitan Police Service (MPS) to his request for an internal review.

13. In response to correspondence from the Commissioner, and having had the opportunity to consider the MPS's internal review response, the complainant confirmed on 9 November 2010 that he wished to pursue his complaint.

14. The Commissioner wrote to the complainant on 23 November 2010 confirming that, although it now appeared he was seeking different information to that originally requested, the scope of his investigation would be the complainant's request for information of 24 November 2009. He further confirmed that, given the wording of that request, the focus of his investigation would be to determine whether the MPS was correct to apply section 40(2) to withhold information within the scope of the request. In this respect, the Commissioner considers that the wording of the request defines the scope.

Chronology

15. The Commissioner commenced his investigation on 9 November 2010.

16. The Commissioner wrote to the MPS on 9 November 2010 asking it for further explanation of its reasons for citing sections 40(2), 30(1)(a)(i) and (ii), 30(1)(b) and (c), 23(5) and 24(2), including its reasons, where appropriate, for concluding that the public interest in maintaining the exemptions outweighed the public interest in disclosure of the information requested.

17. In response to correspondence from the Commissioner on 9 November 2010, the complainant immediately confirmed that he wished to pursue his complaint. Having had the opportunity to consider the MPS's internal review response, the complainant specifically asked the Commissioner to consider the following points:

> *"The response did not satisfy me.*
>
> *For instance, I'm interested in data that would not identify any person (I'm happy for any identifying information to be removed). I would like to know why people were arrested when the politicians were saying the legislation was only for use against terrorists and similar threats: what guidance the police were given or gave (note that while such guidance would relate to the situation, it isn't specific to any individual), whether there was any suggestion anyone arrested appeared to be a serious threat, whether the police decided to use the legislation in situations the politicians said it wouldn't be used."*

18. In view of this, the Commissioner sought an informal resolution in this case.

19. Having been made aware of the complainant's comments, the MPS contacted the complainant on 22 November 2010. Regarding the general circumstances in which the law (RIPA) operates, it provided him with links to a range of information on RIPA, together with links to Parliamentary reports and some statements about conviction data.

20. However, an informal resolution did not prove possible and the complainant contacted the Commissioner on 23 November 2010 confirming that he still wished to pursue his complaint.

21. Following the attempt at informal resolution, on 6 January 2011 the MPS provided the Commissioner with its substantive response to the matters he raised in his correspondence of 9 November 2010. It provided further arguments on 13 January 2011 and 20 January 2011.

Analysis

Exemptions

Section 40(2) Personal information

22. Section 40(2) of the Act is an absolute exemption which relates to the personal information of persons other than the requestor.

23. Section 40(2) together with the condition in section 40(3)(a)(i) or 40(3)(b) provides an absolute exemption if disclosure of information falling within the definition of personal data contained in section 1(1) of the Data Protection Act 1998 (the DPA) would breach any of the data protection principles. A full copy of the section can be found in the Legal Annex at the end of this Decision Notice.

24. In order to reach a view on the MPS's arguments in relation to this exemption, the Commissioner has first considered whether the withheld information is the personal data of one or more third parties.

Is the information personal data?

25. The two main elements of personal data, as defined in section 1(1) of the DPA, are that the information must 'relate' to a living person and that the person must be identifiable. Information will relate to a person if it is about them, linked to them, has some biographical significance for them, is used to inform decisions affecting them, has them as its main focus or impacts on them in any way. The information can be in any form, including electronic data, images and paper files or documents.

26. In this case, the complainant has requested "*all information relating to people convicted under the refusal to decrypt legislation*". In explaining its reasoning for citing section 40(2) in this case, the MPS told the complainant that it has taken the word "all" in his request:

> *"to include details such as witness, victim and accused statements, crime reports, informant information, intelligence, investigating officers report and many other information that is built up during the process of an investigation that leads to an eventual conviction".*

27. Having considered the nature of the withheld information, the Commissioner is satisfied it constitutes information that falls within the definition of 'personal data' as set out in section 1(1) of the Data Protection Act 1998. He has reached this conclusion on the basis that the information comprises personal data relating to the convicted

individual as well as the personal data of other individuals involved in the investigation and proceedings.

28. Further, he is satisfied that the withheld information in its entirety can be considered to be the personal data of the convicted individual as the reason for its very existence is the investigation which led to the conviction.

29. The Commissioner is therefore satisfied, because of the way the request is framed and on the basis of the MPS's representations, that section 40 is engaged.

Is the information sensitive personal data?

30. Sensitive personal data is defined in section 2 of the DPA. It is personal data which falls into one of the categories set out in section 2 of the DPA.

31. The MPS has confirmed that, at the time of the request, it held information about one conviction in relation to the offence of failing to disclose the key to protected information. In this case, the Commissioner considers the relevant category is paragraph (g):

> *"the commission or alleged commission by him of any offence".*

32. The Commissioner is satisfied that the requested information in this case satisfies the definition of sensitive personal data under section 2(g) in relation to the convicted individual.

33. Having accepted that the information requested constitutes the personal data, and in some cases the sensitive personal data, of a living individual other than the applicant, the Commissioner must next consider whether disclosure would breach one of the data protection principles.

Will disclosure breach one of the Data Protection principles?

34. The Commissioner has considered whether disclosure of the requested information would breach any of the data protection principles as set out in schedule 1 of the Data Protection Act (DPA). He considers the most relevant principle in this case to be the first principle which states that:

> *"Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –*
>
> > *(a) at least one of the conditions in Schedule 2 is met, and*
> > *(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met".*

Would it be fair to disclose the requested information?

35. In answering the question of fairness, the Commissioner must take account that disclosure under the Freedom of Information Act is effectively an unlimited disclosure to the public at large, without conditions. When deciding whether or not the information requested in this case is suitable for disclosure, he recognises the importance of considering whether the data subject has consented to the disclosure and/or whether the data subject has actively put some or all of the requested information into the public domain.

Has the data subject consented to the disclosure?

36. The Commissioner notes that there is no obligation on a public authority to seek the data subject's consent to disclosure. However, he considers it good practice to inform the data subject that a request for access to information about them has been made and to take any objections into account.

37. In this case, the Commissioner is not aware of anything to suggest that consent has been given for disclosure of the requested information. The MPS has argued that:

> *"it is quite reasonable to infer that the individual would have no 'reasonable expectation' that sensitive personal information, held by the MPS for the purposes of a criminal investigation, and relating to their alleged commission of offences would be disclosed by the MPS for any other purpose than as part of the criminal justice process, and that consent would not be given."*

38. The MPS has also argued that it is reasonable to suppose that any approach to the data subject asking for permission for disclosure in circumstances where he would be identified and where he can exercise no influence or control over what then happens to his sensitive personal data:

> *"would not only be refused by the subject, but would actively cause him distress."*

Has the data subject actively put some or all of the requested information into the public domain?

39. Where the data subject themselves has put some or all of the requested information into the public domain, the Commissioner considers this weakens the argument that disclosure would be unfair.

40. The Commissioner is aware that an article was published around the time of the request about an individual convicted for refusing to decrypt files. However, as the Commissioner is not aware of any evidence to suggest that the data subject in this case was responsible for some or all of the information contained in the article, he is unable to conclude with any degree of confidence that the data subject in this case provided any input to this article.

41. The Commissioner is also aware that details of the conviction were reported at the time. The Commissioner therefore accepts that there has been some media coverage relating to the case. He accepts that it could therefore be argued that, as some of the withheld information is in the public domain, this reduces the expectation of privacy in this case.

42. However, he is satisfied that this small amount of information in the public domain amounts to media coverage of issues of the day rather than results from the data subject themselves actively putting information about the case into the public domain.

43. Having both considered the nature of the withheld information and looked at the information that was in the public domain at the time of the request, the Commissioner is satisfied that the data subject has not actively sought to put information relevant to the scope of the request into the public domain.

Consequences of disclosure on the data subject

44. The Commissioner considers that the focus of the consequences of disclosure on the harm or distress to the individual should relate to the impact on the individual in a personal capacity.

45. The Commissioner is of the opinion that disclosing personal data is generally less likely to be unfair in cases where the personal data relates to an individual's public or professional life rather than to their private life. The threshold for releasing professional information will generally be lower than that in releasing information relating to an individual's private or home life.

46. In this case the withheld information relates to an individual's private life and, more specifically, to the circumstances of the investigation of that individual.

47. When considering the consequences of disclosure on the data subject, the Commissioner has taken into account the nature of the withheld information itself. He has also considered the fact that disclosure under freedom of information legislation is disclosure to the public at large and not just to the complainant.

48. In this respect, he considers it could reasonably be argued that disclosure of the withheld information in this case has the potential to cause the individual harm or distress.

Conclusion

49. The Commissioner notes that the information in this case falls under section 2(g) of the Data Protection Act 1998 as it relates to the data subject's commission or alleged commission by him of any offence. As such, by its very nature, this has been deemed to be information that individuals regard as the most private information about themselves. Further, as disclosure of this type of information is likely to have a detrimental or distressing effect on the data subject, the Commissioner considers that it would be unfair to disclose the requested information.

50. As the Commissioner has concluded that it would be unfair to the individual concerned to disclose the withheld information and to do so would contravene the first principle of the DPA, he has not gone on to consider whether disclosure would be lawful or whether one of the Schedule 2 DPA conditions would be met. However, his initial view is that no Schedule 2 condition would be met.

51. As section 40 is an absolute exemption there is no need to consider the public interest in disclosure separately.

Other exemptions

52. As the Commissioner has found that it would not be fair to disclose the requested information, he has not gone on to consider the other exemptions cited by the MPS in this case.

53. However, he notes that the MPS is also citing section 30(1) (investigations and proceedings) with respect to the withheld information in this case. In order for the exemption in section 30(1) to be applicable the information must be held for a specific or particular investigation, not for investigations in general, and it continues to be applicable even after an investigation has been completed.

54. In the Commissioner's view, this strengthens the argument that the withheld information in this case is the sensitive personal data of an individual.

Procedural Requirements

55. In this case, the complainant's request was received by the MPS on 24 November 2009 but the MPS did not issue its refusal letter until 12 February 2010. It therefore took the MPS more than 50 working days to respond to the information request. Accordingly, the Commissioner finds

that, in failing to confirm or deny within 20 working days whether it held the requested information, the MPS breached the requirements of section 10(1), and that it also breached section 17(1) by failing to provide the details required by that section within 20 working days.

The Decision

56. The Commissioner's decision is that the public authority dealt with the following elements of the request in accordance with the requirements of the Act:

- it properly withheld the information by reference to the section 40(2) exemption.

57. However, the Commissioner has also decided that the following elements of the request were not dealt with in accordance with the Act:

- the public authority breached section 10(1) by failing to inform the complainant whether it held the requested information within 20 working days of the request; and

- it breached section 17(1) by failing to issue the refusal notice within the statutory time limit.

Steps Required

58. The Commissioner requires no steps to be taken.

Right of Appeal

59. 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,
Arnhem House,
31, Waterloo Way,
LEICESTER,
LE1 8DJ

Tel: 0845 600 0877
Fax: 0116 249 4253
Email: informationtribunal@tribunals.gsi.gov.uk.
Website: www.informationtribunal.gov.uk

60. 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.

61. Any Notice of Appeal should be served on the Tribunal within 28 (calendar) days of the date on which this Decision Notice is sent.

Dated the 3rd day of March 2011

Signed ……

Jon Manners
Group Manager
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Legal Annex

Section 40 Personal information

Section 40(2) provides that –

"Any information to which a request for information relates is also exempt information if-

(a) it constitutes personal data which do not fall within subsection (1), and

(b) either the first or the second condition below is satisfied."

Section 40(3) provides that –

"The first condition is-

(a) in a case where the information falls within any of paragraphs (a) to (d) of the definition of "data" in section 1(1) of the Data Protection Act 1998, that the disclosure of the information to a member of the public otherwise than under this Act would contravene-

(i) any of the data protection principles, or

(ii) section 10 of that Act (right to prevent processing likely to cause damage or distress), and

(b) in any other case, that the disclosure of the information to a member of the public otherwise than under this Act would contravene any of the data protection principles if the exemptions in section 33A(1) of the Data Protection Act 1998 (which relate to manual data held by public authorities) were disregarded."

The Data Protection Principles:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.