

## Freedom of Information Act 2000 (Section 50)

### Decision Notice

Date: 20 January 2011

**Public Authority:** Hampshire Constabulary  
**Address:** Police Headquarters  
West Hill  
Romsey Road  
Winchester  
Hampshire  
SO22 5DB

#### Summary

---

The complainant requested information relating to people convicted under the refusal to decrypt legislation. Hampshire Constabulary neither confirmed nor denied that it holds information, citing the exemptions in sections 40(5) (personal information), 23(5) (information supplied by, or concerning security bodies), 24(2) (national security), 31(3) (law enforcement) and 38(2) (health and safety). The Commissioner has investigated and found the public authority correctly relied on section 40(5). He requires no steps to be taken.

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

3. 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.
4. RIPA regulates the manner in which certain public bodies may conduct surveillance and access a person's electronic communications. For example, the Act enables certain public bodies to demand that someone hands over cryptographic keys to encrypted digital data.
5. 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

---

6. The complainant wrote to Hampshire Police 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/](http://www.theregister.co.uk/2009/11/24/ripa_jfl/)."*
7. Hampshire Police sought clarification the same day, 24 November 2009, asking the complainant to provide additional details about the information he was seeking when he referred in his request to "*all information*". (By virtue of section 1(3) of the Act, the usual 20 working day time limit does not apply where a public authority "*reasonably requires further information in order to identify and locate the information requested*".)
8. Having sought clarification, Hampshire Police responded to the request on 19 January 2010. In its response, it described the request as follows:
  - Point 1 Additional specific and detailed information relating to a case, the basic details of which have appeared in a newspaper article; and
  - Point 2 The number of individuals convicted in Hampshire under the refusal to decrypt legislation.
9. With respect to point 1, it neither confirmed nor denied that it held the information, citing the exemptions in sections 40(5), 30(3), 23(5), 24(2), 38(2) and 31(3) of the Act.
10. With respect to point 2, it told the complainant that "*Hampshire Constabulary does not hold this information as the answer is zero*".

11. The complainant requested an internal review on 19 January 2010 with respect to the decision neither to confirm nor deny that the information referred to as Point 1 was held. In this correspondence, he confirmed that he was happy for identity information such as name and address to be excluded.
12. Hampshire Constabulary upheld its decision neither to confirm nor deny that it held information within the scope of the request in its internal review response of 15 February 2010. In this correspondence, it highlighted parts of the clarification provided by the complainant on 24 November 2009, explaining that it was these elements which led it to continue neither to confirm nor deny that information was held. The Commissioner has reproduced the clarification, as highlighted by Hampshire Constabulary, below:

*"I'm seeking information about what happened; whether it was indeed as the article appeared to report; **whether for example there was any significant risk of terrorist attack from any of the individuals convicted and what evidence there was for this; what matter.** I was mostly interested in the case mentioned in the article, but would like to know of any others.*

*Dates from when the legislation was brought into force to present, but again mostly that where JFL was served with a section 49 notice, **and any interviews that may have been conducted at Fareham station (it wasn't clear from the article whether any had, which is part of the reason I'm making a fairly broad request) or anywhere else you might hold information for.***

*I don't need details like name or address or similar irrelevant personal details, but would like to **know what regard was taken of the mental health of JFL** as I think that is relevant to the appropriateness of the legislation compared to what MPs said it would be for".*

13. On this basis, the Commissioner understands that Hampshire Constabulary considered the requested information relates to:
  - whether there was any significant risk of terrorist attack from any of the individual(s) convicted under the legislation and what evidence there was for this;
  - whether any interviews concerning the individual referred to in the article were conducted at Fareham police station; and
  - whether the mental state of the individual referred to in the article was considered during the course of any investigation.

## The Investigation

---

### Scope of the case

14. Following earlier correspondence, the complainant contacted the Commissioner on 3 June 2010 to confirm that he wished to pursue his complaint about the way his request for information had been handled.
15. The complainant argued that, as he does not "*need or want personally identifying information*", Hampshire Constabulary's refusal to confirm or deny is not appropriate.
16. The Commissioner told the complainant in correspondence that, unless he heard from him to the contrary, the scope of his investigation would be to determine whether or not Hampshire Constabulary was correct neither to confirm nor deny whether it held the information referred to as Point 1 in its correspondence of 19 January 2010 and highlighted in bold in its correspondence of 15 February 2010. As the Commissioner did not hear anything back from the complainant, he has undertaken his investigation on that basis.
17. Having taken account of the nature of the requested information which, if it were held, would fall within the scope of his investigation, the Commissioner considers that it would constitute personal data, and in some respects sensitive personal data, about a third party.
18. The Commissioner explained to the complainant that he has previously addressed the issue of confirming or denying whether personal data is held. He advised accordingly on the likely outcome of his investigation. Nevertheless, the complainant required the Commissioner to issue a Decision Notice in this case.
19. The Commissioner has therefore proceeded to address this case in light of his established position with regard to the confirmation or denial of the holding of personal information.

### Chronology

20. The Commissioner wrote to Hampshire Constabulary on 27 August 2010 asking it for further explanation of its reasons for neither confirming nor denying that it holds information within the scope of Point 1 of the request.
21. Hampshire Constabulary provided a comprehensive response on 30 September 2010.

## Analysis

---

### Exemptions

#### **Section 40 Personal information and the exclusion from the duty to confirm or deny**

22. Generally, the provisions of section 40(1) to (4) exempt 'personal data' from disclosure under the Act if to do so would breach the data protection principles. In relation to a request which constitutes the personal data of individual(s) other than the applicant(s), as in this case, section 40(5)(b)(i) further excludes a public authority from complying with the duty imposed by section 1(1)(a) if complying with that duty would contravene any of the data protection principles, or section 10 of the Data Protection Act 1998 (the "DPA"), or would do so if the exemptions in section 33A(1) of that Act were disregarded.
23. A full text of section 40 can be found in the Legal Annex at the end of this Decision Notice.
24. Therefore, when determining in this case whether or not Hampshire Constabulary was correct neither to confirm nor deny that information is held on the basis that section 40(5)(b)(i) applied, the Commissioner must consider the following questions.
  - Would confirming or denying whether information is held constitute a disclosure of personal data? If so, whose personal data?
  - If confirming or denying would involve the disclosure of personal data, would this contravene any of the data protection principles and, if so, which ones and why?

#### ***Would confirming or denying whether information is held constitute the disclosure of personal data? If so, whose personal data?***

25. Personal data is defined in section 1(1) of the Data Protection Act (DPA) as:

*"data which relate to a living individual who can be identified-*

*(a) from those data, or*

*(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,*

*and includes any expression of opinion about the individual and any indication of the intention of the data controller or any other person in respect of the individual”.*

26. In the Commissioner’s view, the two main elements of personal data are that the information must “relate to” a living person, and that 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.
27. In this case, the request refers specifically to an individual who has been written about in an article. In this instance, there is no reason to believe that the individual is deceased and therefore information, if held, would relate to a living individual. Although the individual is not named, the Commissioner’s view is that simply because the name of an individual is not known does not mean that the individual cannot be identified.
28. 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, ie personal data consisting of information as to:

*“...*

*(a) the racial or ethnic origin of the data subject,*

*(b) his political opinions,*

*(c) his religious beliefs or other beliefs of a similar nature,*

*(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),*

*(e) his physical or mental health or condition,*

*(f) his sexual life,*

*(g) the commission or alleged commission by him of any offence,*

*(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings”.*

29. In this case, the clarified request asks about convicted individual(s), the location of interviews and what consideration was given to the mental health of an individual. Due to the nature of the information requested such information would, if held, reveal information about the commission or alleged commission by an individual of an offence as well as about their mental health.

30. The Commissioner therefore considers subsections (e) and (g) to be relevant. He is satisfied that all of the information within the scope of the request would, if held, fall within the definition of sensitive personal data as defined above.

***Would confirming or denying whether information is held contravene any of the data protection principles?***

31. The Commissioner has next considered whether or not confirming or denying information is held would contravene any of the data protection principles.

*The first data protection principle*

32. The Commissioner considers the first data protection principle to be the relevant one in this case. This 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 DPA 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'.*

33. As he is satisfied that all of the information pertinent to the request would, if held, constitute sensitive personal data, the Commissioner must consider the criteria that have to be met in order for sensitive personal data to be disclosed under the Act.
34. The Commissioner's approach when considering whether sensitive personal data should be disclosed under the Act is to begin by considering whether any of the conditions in schedule 3 can be met.
35. Having considered the conditions listed in schedule 3, and in particular those in paragraphs 1 and 5, the Commissioner has formed the view that none of these conditions can be met. (The text of paragraphs 1 and 5 from the schedule can be found in the Legal Annex at the end of this Decision Notice).
36. The Commissioner is satisfied that the exemption in section 40(5)(b)(i) of the Act is engaged in this case and provides an exemption from confirming or denying that information is held. This is because the effect of complying with section 1(1)(a), by either confirming or denying that information is held, would constitute the disclosure of an identifiable individual's sensitive personal data. This would breach the first data protection principle because none of the conditions in Schedule 3 can be met.

37. As the Commissioner has decided that a schedule 3 condition for the disclosure of this information cannot be met, and that disclosure would therefore be in breach of the first principle of the DPA, he has not gone on to consider whether there is a schedule 2 condition or whether disclosure would be fair or lawful.
38. Since section 40(5)(b)(i) is an absolute exemption, no public interest test applies.

### **The public domain issue**

39. While the Commissioner takes the view that most exemptions under the Freedom of Information Act will not usually apply to information which is in the public domain, that general position does not apply to information which constitutes personal data (and is therefore subject to section 40). The reason is that personal data is subject to the separate legal regime of the Data Protection Act, which focuses on legitimate 'processing'.
40. The Commissioner is aware that an article has been published about an individual convicted under the RIPA legislation and that this event is the subject of the request. However, in relation to the information requested by the complainant, the Commissioner is not aware of any relevant information being attributed to Hampshire Constabulary or of Hampshire Constabulary having issued a press statement or public briefing in relation to this matter.
41. As the Commissioner has determined that a schedule 3 condition cannot be satisfied in this case, confirming or denying that this information exists would result in Hampshire Constabulary being in breach of the DPA. This is because confirmation or denial would reveal sensitive personal data, namely with respect to:
  - whether there was a significant risk of terrorist attack from any of the individual(s) convicted and what evidence there was for this;
  - where interviews about an alleged offence took place; and
  - what regard was taken of the mental health of an individual.



### **Other exemptions – sections 23, 24, 30, 31 and 38**

42. Since the Commissioner has concluded that Hampshire Constabulary cited section 40(5)(b)(i) of the Act appropriately he does not propose to reach any conclusion in this Decision Notice regarding its application of the exemptions in sections 23, 24, 30, 31 and 38.

### **The Decision**

---

43. The Commissioner's decision is that the public authority correctly relied on section 40(5)(b)(i) to refuse to confirm or deny whether it held the requested information.

### **Steps Required**

---

44. The Commissioner requires no steps to be taken.

## Right of Appeal

---

45. 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](mailto:informationtribunal@tribunals.gsi.gov.uk).

Website: [www.informationtribunal.gov.uk](http://www.informationtribunal.gov.uk)

46. 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.
47. 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 20<sup>th</sup> day of January 2011**

**Signed .....**

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

## Legal Annex

---

### **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.”

### **Data Protection Act - Schedule 3**

“Conditions relevant for purposes of the first principle: processing of sensitive personal data.

1. The data subject has given his explicit consent to the processing of the personal data.
5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.”