

Freedom of Information Act 2000 (Section 50)

Decision Notice

Date: 27 May 2010

Public Authority: The Cabinet Office
Address: 70 Whitehall
London
SW1A 2AS

Summary

The complainant requested the email address of an individual who had contributed to a public consultation about Building Britain's Future. The public authority responded that this information was that individual's personal data, that the disclosure of it would be unfair to that individual and that it can appropriately rely on section 40(2) in this case. It reaffirmed its decision in its internal review.

The Commissioner has considered this case and finds that the information has been withheld appropriately by virtue of section 40(2). He therefore dismisses the complaint. He has however found procedural breaches of sections 10(1) and 17(1). He requires no remedial 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. The public authority ran a website called Building Britain's Future. It asked the public to provide their comments by email about a selection of topics.

3. The website began by recommending that 1000 characters were written. However, it would allow more than 1000 characters to be entered. It was then changed to allow only 1000 characters.
4. Before this change occurred an individual provided a submission and wrote 1284 characters. It was about historic Youth Training Scheme (YTS) issues and about the need for benefits to assist only those who cannot work.
5. The complainant was unhappy that this individual could use more than 1000 characters and asked for their email address. The subject of this case is that email address.

The Request

6. After a few exchanges of emails the complainant requested the following information on 8 July 2009:

'What is [individual redacted] 's email address? Emails are requested'

7. On 7 August 2009 the complainant wrote a reminder:

'I have not received [Individual Redacted] 's email address, requested on 8th July. I understand that such personal information has to be disclosed, where disclosure is in the public interest and does not harm the interests of the individual involved, which applies in this case.'

8. On 10 August 2009 the complainant also requested an internal review of the delay to be conducted.
9. On 28 September 2009 the public authority wrote to the complainant to ask for clarification about what it was that it was required to review. It also apologised for the delay.
10. The complainant replied on the same day and explained that he wanted the request for the email address to be answered.
11. On 30 September 2009 the public authority acknowledged the receipt of the request.
12. On 12 November 2009 the complainant complained again that he had not received an appropriate response.

13. On 17 November 2009 the public authority issued a response. It stated that it held the individual's email address but it was withholding it. It explained that it believed that section 40(2) of the Act applied. This was because it was personal data and disclosure of it would contravene the data protection principles under the Data Protection Act.
14. On 18 November 2009 the complainant requested an internal review. He explained that he was dissatisfied with the time taken and that he was not happy about the verdict. He explained:

'It is not clear that [Individual redacted]'s email address is personal data, because data is only personal if it is possible to identify the individual from the data. Even if it is personal data, it must be disclosed if "disclosure is necessary for a legitimate public interest with no unwarranted harm to the individual's interests."

http://www.ico.gov.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/personal_information.pdf

'There is a legitimate public interest in demonstrating that the responses to the consultation about Britain's future do not come from the Cabinet Office. Disclosing [Individual Redacted]'s email address will not harm his interests.'

15. On 20 November 2009 the complainant provided further submissions:

'I have read in the link in my email of 18th November that you have "a duty to confirm or deny whether you hold the information". I was informed by the email of [Employee redacted] of 8th July, that the Cabinet Office does not know who [individual redacted] is. Therefore this cannot be personal information from the point of view of the Data Protection Act 1998.'

16. On 4 January 2010 the complainant wrote a reminder to the public authority and explained that his internal review was taking too long.

The Investigation

Scope of the case

17. On 6 January 2010 the complainant contacted the Commissioner to complain about the way his request for information had been handled. The complainant specifically asked the Commissioner to consider the following points:
 - He was restricted to 1000 characters in the consultation and was concerned why someone else was not.
 - He was concerned about the delays in receiving a response.
 - He was concerned about the delays in acquiring internal review and had already provided a reminder.
18. The outstanding information is the email address itself. This has been confirmed throughout all the correspondence since 7 August 2009.
19. The Commissioner's remit only concerns information access matters. He is not the body to adjudicate whether consultation contributions should have a uniform number of characters.

Chronology

20. 18 January 2010: The Commissioner wrote to the public authority to remind it about conducting internal reviews in line with his guidance and asked it to conduct an internal review within twenty working days. He also wrote to the complainant to explain those actions and also invited him to contact the Commissioner in the event that the internal review was not provided by then.
21. 22 February 2010: The complainant responded to the Commissioner and informed him that he was still to receive a response to his request for an internal review.
22. 2 March 2010: The Commissioner wrote to the public authority to explain that he had received an eligible complaint as the public authority had not communicated the results of its internal review.
23. 18 March 2010: The Commissioner telephoned the public authority about this complaint. He explained that given the delay in this case he was prepared to investigate the case without an internal review. He asked the public authority either to conduct its internal

- review promptly or tell the Commissioner it was prepared to waive the right to conduct an internal review. He also asked to receive a copy of the withheld information and confirmed what was said in the conversation by email.
24. 25 March 2010: The Commissioner was telephoned by the public authority who explained that it wanted to conduct an internal review.
 25. 31 March 2010: The complainant called the Commissioner about the progress of this case. The Commissioner explained that it was likely that a Decision Notice would need to be issued.
 26. On 31 March 2010, 6 April 2010, 9 April 2010, 14 April 2010 and 21 April 2010 the Commissioner telephoned the public authority to ask why the internal review was not conducted and was told various things.
 27. 21 April 2010: The Commissioner emailed the public authority again. He once again asked for the internal review to be conducted and for a copy of the withheld information. He also used the opportunity to make further enquiries about the public authority's position.
 28. On 4 May 2010 and 6 May 2010 the Commissioner telephoned the public authority again to ask why there had been no progress.
 29. 6 May 2010: The public authority issued its internal review response to the complainant. It explained that it upheld its original position for the same reasons as in its refusal notice. It explained that it believed that the disclosure of the information would not be fair to the data subject or lawful and therefore section 40(2) applied.
 30. The public authority also provided the Commissioner with both the withheld information and the answers to the enquiries that he made on 21 April 2010.
 31. 7 May 2010: The Commissioner wrote to the data subject of the email address to invite the individual to make submissions in this case should they want to. The individual failed to respond.
 32. 19 May 2010: The Commissioner spoke to the complainant to ensure that he wanted this case to continue.

Analysis

Exemption

Section 40(2)

33. The public authority has argued that disclosure of an email address would involve disclosing the personal data of a living individual. It then stated that it believed that it would contravene one of the data protection principles of the Data Protection Act 1998 ("DPA"). As such it would be exempt from disclosure under section 40(2) by virtue of section 40(3)(a)(i). Section 40 is set out in full in a Legal Annex to this notice.
34. The complainant argued that the individual was not identifiable from their email address and therefore the information did not constitute personal data. Alternatively the email address was not personal data because the public authority did not know who the individual was. He explained that even if the information was personal data in his view the legitimate interest in knowing that the consultation response did not come from the public authority outweighed the individual's rights to privacy in this case.
35. The public authority's main arguments centred on the application of the first data protection principle. It believes that disclosure of the personal data in question would be unfair and would not satisfy one of the conditions for processing listed in Schedule 2 of DPA. These arguments are considered in more detail below.
36. It is important to note that any disclosure under this Act is disclosure to the public at large and not just to the complainant. If the public authority is prepared to disclose the requested information to the complainant under the Act it should be prepared to disclose the same information to any other person who asks for it. The Tribunal in the case of *Guardian & Brooke v The Information Commissioner & the BBC* (EA/2006/0011 and EA/2006/0013) (following *Hogan and Oxford City Council v The Information Commissioner* (EA/2005/0026 and EA/2005/0030)) confirmed that, "*Disclosure under FOIA is effectively an unlimited disclosure to the public as a whole, without conditions*" (paragraph 52):
http://www.informationtribunal.gov.uk/Documents/decisions/guardian_news_HBrooke_v_infocomm.pdf.
37. In analysing the application of section 40(2), the Commissioner considered a) whether the information in question was personal data

and b) whether disclosure of the personal data under the Act would contravene the first data protection principle.

Is the information personal data?

38. Personal data is defined in section 1 of 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 intentions of the data controller or any other person in respect of the individual.'

39. When considering whether the information is personal data, the Commissioner had regard to his own published guidance: "Determining what is personal data" which can be accessed at:

http://www.ico.gov.uk/upload/documents/library/data_protection/related_specialist_guides/personal_data_flowchart_v1_with_preface001.pdf

40. From his guidance there are two questions that need to be answered in the affirmative when deciding whether the information if disclosed to the public would constitute the personal data of individuals:

(i) Can a living individual be identified from the data, or, from the data and other information in the possession of, or likely to come into the possession of, the members of the public?

(ii) Does the data 'relate to' the identifiable living individual, whether in personal or family life, business or profession?

41. The Commissioner notes that the withheld information in this case amounts to the email address of an individual. Without prejudicing the integrity of the information, the Commissioner can also confirm that the email address includes elements of the name of that individual.

42. The question to be determined is whether a living individual can be identified from that data if the information is disclosed to the public.

43. The Commissioner considers that truly anonymised data is not personal data and there would be no need to consider the application of the data

protection principles. The Commissioner considers that even where the data controller holds the additional 'identifying' information, this does not prevent them from anonymising that information to the extent that it would not be possible to identify any living individual from that information alone and thus it would no longer be personal data when released. The test of whether information is truly anonymised is whether a member of the public could identify a living individual by cross-referencing the data with information or knowledge already available to the public. This approach is supported by paragraphs 24 and 25 of Lord Hope's judgement in the House of Lords' case of the *Common Services Agency v Scottish Information Commissioner* (2008) UKHL 47:

"..Rendering data anonymous in such a way that the individual to whom the information from which they are derived refers is no longer identifiable would enable the information to be released without having to apply the principles of [data] protection."

44. The Commissioner does not consider that the withheld information in this case to be truly anonymous. The reason for this is that firstly the email address contains elements that are components of an individual's name. Secondly, any member of the public can contact an individual through their email address and this shows that it can be linked with ease to a specific individual. Therefore revealing the email address is likely to reveal information that can be tied to a specific individual and would therefore constitute a release of personal data.
45. The Commissioner has no reason to believe that the individual is dead and the information is therefore about a living individual.
46. In the light of the analysis above, the Commissioner is therefore satisfied that the email address of an individual relates to them and constitutes their personal data. He believes that this is the case as a general rule and that this is so in this case.

Would disclosure of the personal data under the Act contravene the first data protection principle?

47. The first data protection principle has two main components. These are as follows:
 - A requirement to process all personal data fairly and lawfully; and
 - A requirement to satisfy at least one DPA Schedule 2 condition for processing of all personal data.

48. Both requirements must be satisfied to ensure compliance with the first data protection principle. If even one requirement cannot be satisfied, processing will not be in accordance with the first data principle.

Would disclosure be fair and lawful?

49. In considering whether disclosure of this information would be unfair and therefore contravene the requirements of the first data protection principle, the Commissioner has taken the following factors into account:
- The individual's reasonable expectations of what would happen to their personal data and whether disclosure would be incompatible with the purposes for which it was obtained;
 - Whether disclosure would cause any unnecessary or unjustified damage and/or distress to the individual; and
 - Legitimate interests of the public in knowing the email address of a member of the public who contributed to a consultation.
50. The Commissioner has considered the data subject's reasonable expectations in this case. In order to do so, he has considered the Building Britain's Future privacy policy. This explained that the public authority 'do not pass on your details to any third party or other government department'¹. This policy is clear and unambiguous and the Commissioner believes that the reasonable expectations of an individual when he makes a submission on the consultation would be that his email address and any other personal details would not be passed to any third party. Indeed, if those details were not protected in accord with its policy then people may be discouraged from contributing to the consultation and in the Commissioner's view this would make the disclosure incompatible with the purposes for which the details were obtained.
51. The Commissioner has also considered the architecture of the website and believes that the way it is structured is designed to protect individuals from having their views attacked by others. Indeed the way that it provides such protection will enable views to be expressed freely and frankly. Free and frank views are necessary for the consultation to proceed in a manner that is useful to the public authority and by extension to the public. The Commissioner believes that the architecture of the website strengthens further the reasonable

¹ <http://www.cabinetoffice.gov.uk/privacy.aspx> (as at 17 May 2010)

expectations of the data subject that the email address would not be disclosed.

52. The Commissioner is satisfied that the disclosure of this email address invites the possibility of causing unjustified damage or distress to the data subject. They provided their contact details on the understanding both implicit and explicit that this information would not be disclosed to the public. An email address is an important means of correspondence for an individual and the sending of unwanted, personal email messages represents an intrusion into the recipients' private life. The way in which the law protects against unsolicited marketing messages is evidence of this.² Disclosure of the email address would open the data subject up to the possibility of unwelcome, and possibly distressing, email messages.
53. When considering the legitimate interests of the public the Commissioner has started from the position that there is an underlying benefit in transparency and accountability where possible. Indeed, the purpose of the Act is to provide information that would contribute to a more open society.
54. However, the Commissioner is of the view that the provision of the email address would not contribute to public understanding of whether the consultation process was fair. He does not believe that it is necessary and believes it does not come close to justifying the intrusion to the data subject in this case.
55. In addition, the Commissioner has considered the complainant's argument about the necessity to know that the Cabinet Office do not contribute to their own consultation. He notes that in any event, the YTS scheme was not managed by the Cabinet Office. Instead it was coordinated by the Manpower Services Commissioner. The Commissioner is of the view that a public consultation should be available to all members of the public, wherever they work. The idea is to have a diversity of viewpoints so that the best ideas can influence policy. He has also considered the issue that the individual had more characters to make his point, than the suggested maximum (that was subsequently imposed) and believes that this factor is irrelevant to the legitimate interests of the public in this case.
56. Therefore when considering how the factors balance, the Commissioner has come to the conclusion that the disclosure of the requested information would be unfair to the data subject. The central reason for

² Such as in The Privacy and Electronic Communications (EC Directive) Regulations 2003 that are also regulated by the Commissioner.

this conclusion is that the legitimate expectations of the individual are that the information would not be provided and the overriding of these expectations cannot be justified in this case. As the release of the information would be unfair, the first data protection principle would be contravened and the information therefore engages the section 40(2) exemption.

57. The Commissioner therefore upholds the public authority's application of section 40(2) to the withheld information [by virtue of section 40(3)(a)(i)].

Procedural Requirements

Section 10(1)

58. Section 10(1) of the Act (full wording in the legal annex) provides that the public authority must comply with sections 1(1)(a) and 1(1)(b) within twenty working days. In this case the public authority took more than twenty working days and therefore breached section 10(1) twice.

Section 17(1)

59. Section 17(1) also provides that an appropriate refusal notice should be issued in twenty working days. As the public authority failed to do this, it also breached section 17(1).

The Decision

60. 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 correctly withheld the email address by virtue of the section 40(2) exemption in the Act.

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

- It breached section 10(1) twice as it failed to provide an appropriate response within twenty working days.
- It breached section 17(1) as it failed to issue an appropriate refusal notice in twenty working days.

Steps Required

62. The Commissioner requires no steps to be taken.

Other matters

63. There is no timescale laid down in the Act for a public authority to complete an internal review. However, as he has made clear in his *'Good Practice Guidance No 5'*, the Commissioner considers that these internal reviews should be completed as promptly as possible. In the absence of exceptional circumstances, a reasonable time for completing an internal review is 20 working days from the date of the request for review. In exceptional circumstances it may be reasonable to take longer, but the total time taken should not exceed 40 working days, and as a matter of good practice the public authority should explain to the requester why more time is needed.
63. In this case the complainant's internal review request was made on 18 November 2009 and the public authority communicated its decision on 6 May 2010. The public authority therefore took almost six months to complete the review. In addition the Commissioner contacted the public authority more than ten times to remind the public authority to conduct the internal review in this case. The Commissioner does not believe that any exceptional circumstances existed in this case to justify that delay, and he therefore wishes to register his view that the public authority fell short of the standards of good practice in failing to complete its internal review within a reasonable timescale.

Right of Appeal

64. 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

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.

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 27th day of May 2010

Signed

**David Smith
Deputy Commissioner**

**Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF**

Legal Annex

The Freedom of Information Act 2000

Section 1 - General right of access to information held by public authorities

(1) Any person making a request for information to a public authority is entitled—

(a) to be informed in writing by the public authority whether it holds information of the description specified in the request, and

(b) if that is the case, to have that information communicated to him.

(2) Subsection (1) has effect subject to the following provisions of this section and to the provisions of sections 2, 9, 12 and 14.

(3) Where a public authority—

(a) reasonably requires further information in order to identify and locate the information requested, and

(b) has informed the applicant of that requirement,

the authority is not obliged to comply with subsection (1) unless it is supplied with that further information.

Section 10 - Time for compliance with request

(1) Subject to subsections (2) and (3), a public authority must comply with section 1(1) promptly and in any event not later than the twentieth working day following the date of receipt.

(2) Where the authority has given a fees notice to the applicant and the fee is paid in accordance with section 9(2), the working days in the period beginning with the day on which the fees notice is given to the applicant and ending with the day on which the fee is received by the authority are to be disregarded in calculating for the purposes of subsection (1) the twentieth working day following the date of receipt.

(3) If, and to the extent that—

(a) section 1(1)(a) would not apply if the condition in section 2(1)(b) were satisfied, or

(b) section 1(1)(b) would not apply if the condition in section 2(2)(b) were satisfied,

the public authority need not comply with section 1(1)(a) or (b) until such time as is reasonable in the circumstances; but this

subsection does not affect the time by which any notice under section 17(1) must be given.

...

Section 40 – Personal information

(1) Any information to which a request for information relates is exempt information if it constitutes personal data of which the applicant is the data subject.

(2) 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.

(3) 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 [1998 c. 29.] 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 [1998 c. 29.] Data Protection Act 1998 (which relate to manual data held by public authorities) were disregarded.

(4) The second condition is that by virtue of any provision of Part IV of the [1998 c. 29.] Data Protection Act 1998 the information is exempt from section 7(1)(c) of that Act (data subject’s right of access to personal data).

(5) The duty to confirm or deny—

(a) does not arise in relation to information which is (or if it were held by the public authority would be) exempt information by virtue of subsection (1), and

(b) does not arise in relation to other information if or to the extent that either—

(i) the giving to a member of the public of the confirmation or denial that would have to be given to comply with section 1(1)(a) would (apart from this Act) contravene any of the data protection principles or section 10 of the [1998 c. 29.] Data Protection Act 1998 or would do so if the exemptions in section 33A(1) of that Act were disregarded, or

(ii) by virtue of any provision of Part IV of the [1998 c. 29.] Data Protection Act 1998 the information is exempt from section 7(1)(a) of that Act (data subject's right to be informed whether personal data being processed).

(6) In determining for the purposes of this section whether anything done before 24th October 2007 would contravene any of the data protection principles, the exemptions in Part III of Schedule 8 to the [1998 c. 29.] Data Protection Act 1998 shall be disregarded.

(7) In this section—

- “the data protection principles” means the principles set out in Part I of Schedule 1 to the [1998 c. 29.] Data Protection Act 1998, as read subject to Part II of that Schedule and section 27(1) of that Act;
- “data subject” has the same meaning as in section 1(1) of that Act;
- “personal data” has the same meaning as in section 1(1) of that Act.

Data Protection Act 1998

Section 1 - Basic interpretative provisions

(1) In this Act, unless the context otherwise requires—

- “data” means information which—
 - (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
 - (b) is recorded with the intention that it should be processed by means of such equipment,
 - (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, or
 - (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68;
- “data controller” means, subject to subsection (4), a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed;
- “data processor”, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller;

- “data subject” means an individual who is the subject of personal data;
 - “personal data” means 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 intentions of the data controller or any other person in respect of the individual;
 - “processing”, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including—
 - (a) organisation, adaptation or alteration of the information or data,
 - (b) retrieval, consultation or use of the information or data,
 - (c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
 - (d) alignment, combination, blocking, erasure or destruction of the information or data;
 - “relevant filing system” means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.
- (2) In this Act, unless the context otherwise requires—
- (a) “obtaining” or “recording”, in relation to personal data, includes obtaining or recording the information to be contained in the data, and
 - (b) “using” or “disclosing”, in relation to personal data, includes using or disclosing the information contained in the data.
- (3) In determining for the purposes of this Act whether any information is recorded with the intention—
- (a) that it should be processed by means of equipment operating automatically in response to instructions given for that purpose, or

(b) that it should form part of a relevant filing system,

it is immaterial that it is intended to be so processed or to form part of such a system only after being transferred to a country or territory outside the European Economic Area.

(4) Where personal data are processed only for purposes for which they are required by or under any enactment to be processed, the person on whom the obligation to process the data is imposed by or under that enactment is for the purposes of this Act the data controller.