HOUSE OF LORDS SESSION 2007–08

[2008] UKHL 47

on appeal from: [2006] SCOTCS CSIH 58

OPINIONS
OF THE LORDS OF APPEAL
FOR JUDGMENT IN THE CAUSE

Common Services Agency (Appellants) *v* Scottish Information Commissioner (Respondent) (Scotland)

Appellate Committee

Lord Hoffmann
Lord Hope of Craighead
Lord Rodger of Earlsferry
Baroness Hale of Richmond
Lord Mance

Counsel

Appellants:
Valerie Stacey QC
Ruth Crawford

(Instructed by Reynolds Porter Chamberlain LLP for R F Macdonald)

Respondent:
Paul Cullen QC
Morag Ross

(Instructed by Brodies LLP)

First Intervener (Information Commissioner)
Timothy Pitt-Payne
(Instructed by Information Commissioner's Office)

Second Intervener (Secretary of State for Justice)
Lord Davidson of Glen Clova QC
Jason Coppel
John MacGregor

(Instructed by Treasury Solicitors for Office of the Solicitor to the Advocate General)

Hearing date:
1 and 2 APRIL 2008

ON
WEDNESDAY 9 JULY 2008

HOUSE OF LORDS

OPINIONS OF THE LORDS OF APPEAL FOR JUDGMENT IN THE CAUSE

Common Services Agency (Appellants) *v* Scottish Information Commissioner (Respondent) (Scotland)

[2008] UKHL 47

LORD HOFFMANN

My Lords,

1. I have had the advantage of reading in draft the speech of my noble and learned friend Lord Hope of Craighead. For the reasons he gives, with which I agree, I too would allow this appeal.

LORD HOPE OF CRAIGHEAD

My Lords,

2. This case raises important questions about the interaction between provisions of the Data Protection Act 1998 ("DPA 1998") on the one hand and provisions of the Freedom of Information (Scotland) Act 2002 ("FOISA 2002") on the other. The corresponding provisions of the Freedom of Information Act 2000 ("FOIA 2000"), which extends to the whole of the United Kingdom and applies to UK public authorities located in Scotland, are not engaged directly. The appellant, the Common Services Agency ("the Agency"), is a special Health Board the regulation of whose functions is a matter for the Scottish Parliament: see FOIA 2000, section 80. But much of the wording of section 38 of FOISA 2002, which addresses the overlap between rights of access under that Act and rights of access under DPA 1998, is reproduced in section 40 of FOIA 2000, which addresses the same problem. Section 38(2)(a) of FOISA, in particular, is in exactly the same terms as section 40(3)(a) of FOIA 2000. So resolution of these questions will have a

bearing on the interaction between DPA 1998 and freedom of information legislation throughout the United Kingdom.

3. Unlike DPA 1998, which was designed to implement Council Directive 95/46/EC of 25 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, neither FOIA 2000 nor FOISA 2002 were enacted to give effect to the United Kingdom's obligations under community law. But there had been increasing pressure for the enactment of legislation of this kind, reflecting concern about the lack of openness on the part of the executive. The US Freedom of Information Act 1966 was an important landmark, as was the introduction, following Declaration No 17 to the Treaty of Maastricht 1992 that openness is an essential aspect of democracy, in 1994 of a provision giving freedom of information rights to any citizen of the EU enforceable against institutions of the European Community: article 255 EC. The Labour Party came to power in 1997 with a manifesto commitment to introduce a Freedom of Information Act. FOIA 2000 was the product of that commitment. In November 1999, within six months of the commencement of the Scotland Act 1998, the Scottish Executive published a consultation document called "An Open Scotland". This was followed by the publication in March 2001 of a draft Freedom of Information (Scotland) Bill. Section 1(1) of FOISA 2002 resulted from these initiatives. It sets out a general entitlement on the part of any applicant for information from a Scottish public authority which holds it to be given that information. But the general entitlement to that information is qualified by the reference in section 2 to exemptions. An annotation in *Current Law Statutes* describes section 2 as probably the most structurally significant section of the Act.

4. There is much force in Lord Marnoch's observation in the Inner House that, as the whole purpose of FOISA is the release of information, it should be construed in as liberal a manner as possible: [2006] CSIH 58, 2007 SC 231, para 32. But that proposition must not be applied too widely, without regard to the way the Act was designed to operate in conjunction with DPA 1998. It is obvious that not all government can be completely open, and special consideration also had to be given to the release of personal information relating to individuals. So while the entitlement to information is expressed initially in the broadest terms that are imaginable, it is qualified in respects that are equally significant and to which appropriate weight must also be given. The scope and nature of the various exemptions plays a key role within the Act's complex analytical framework.

5. Section 2(1) FOISA 2002 distinguishes between exemptions which are absolute and those which are not. A provision which confers absolute exemption is not subject to a public interest test. Other exemptions are. Among the absolute exemptions is that for "personal data" within the meaning given to that expression by section 1(1) of DPA 1998: FOISA 2002, section 38. According to the Explanatory Notes, p 6, this section is intended to ensure that FOISA does not interfere with DPA 1998. Any information which constitutes personal data of which the applicant is the data subject is exempt from the obligation which section 1 FOISA 2002 imposes on the public authority: section 38(1)(a). The right of the data subject to obtain access to that information is confined to that which the individual is given by sections 7 to 9 DPA 1998. Any information which constitutes personal data other than that of which the applicant is the data subject is also exempt if it satisfies one or other of two conditions which are designed to preserve the application of DPA 1998 to that information. This is the effect of section 38(1)(b), section 38(2) and section 38(3).

6. Section 38(1)(b) FOISA 2002 provides:

> "Information is exempt information if it constitutes –
>
> (b) personal data and either the condition mentioned in subsection (2) (the 'first condition') or that mentioned in subsection (3) (the 'second condition') is satisfied."

The second condition mentioned in section 38(3) is not relevant to this case. The first condition mentioned in section 38(2) takes one or other of two alternative forms, of which the one relevant to this case is set out in section 38(2)(a) (i) as follows:

> "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 (c 29), 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."

The data protection principles are set out in Schedule 1 DPA 1998. The first principle is in para 1 of Schedule 1, which provides:

> "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."

7. In my opinion there is no presumption in favour of the release of personal data under the general obligation that FOISA lays down. The references which that Act makes to provisions of DPA 1998 must be understood in the light of the legislative purpose of that Act, which was to implement Council Directive 95/46/EC. The guiding principle is the protection of the fundamental rights and freedoms of persons, and in particular their right to privacy with respect to the processing of personal data: see recital 2 of the preamble to, and article 1(1) of, the Directive. Recital 34 and article 8(1) recognise that some categories of data require particularly careful treatment. Section 2 DPA 1998, which defines the expression "sensitive personal data", must be understood in the light of this background.

The request and how it was dealt with

8. Among the functions which the Agency performs under the powers that have been given to it by the National Health Service (Functions of the Common Services Agency) (Scotland) Order 1974 (SI 1974/467), as amended, is the collection and dissemination of epidemiological information from other Health Boards. It was with that in mind that on 11 January 2005 Mr Collie, acting on behalf of Chris Ballance who was then a member of the Scottish Parliament, asked the Agency to supply him with details of all incidents of childhood leukaemia for both sexes by year from 1990 to 2003 for all the DG (Dumfries and Galloway) postal area by census ward. There is no doubt that there was, and still is, a genuine public interest in the disclosure of this information. For many years concern has been expressed about risks to public health in the area arising from operations at the MOD's Dundrennan firing range, the now decommissioned nuclear reactor at Chapelcross and the nuclear processing facilities at Sellafield. But the Agency refused Mr Collie's request. He was told that the Agency did not hold these details for 2002 or 2003 as the data relating to these years was still incomplete. As for the earlier years, there was a significant risk of the indirect identification of living individuals due to the low numbers resulting from the combination of the rare diagnosis, the specified age group and the small geographic area. As a result it was personal data within the meaning of section 1(1) of DPA and was exempt information for the purposes of FOISA 2002. The Agency also

maintained that it owed a duty of confidence equivalent to that of the clinicians to whom the information had originally been made available.

9. Mr Collie then applied to the Commissioner under section 47 FOISA 2002 for a decision whether his request for information had been dealt with in accordance with Part I of the Act. The Commissioner provided the parties with an initial draft of his decision. In para 68 he said that he was minded to accept that the data at ward census level constituted personal data. But he saw the task of the Agency as being to establish the level of release which most closely matched that which Mr Collie had requested, while giving an appropriate level of confidence that the data did not represent personal data. He said that at that stage he had in mind the release of the information for each year requested at Health Board level, but this was not acceptable to Mr Collie. On 15 August 2005 the Commissioner issued his decision under section 49(3)(b) FOISA. In para 95 of the decision he said that he was satisfied that a living individual could be identified from the data at census ward level and that it constituted personal data as defined by section 1(1) FOISA 2002. He then turned to Schedule 1 DPA 1998, which sets out the data protection principles with which the Agency had to comply.

10. In paras 101 - 105 of the decision the Commissioner said that he was satisfied that the disclosure of the information requested by Mr Collie would breach the first principle and that it should not be released. Its release could be said to be unlawful if it could be said to constitute a breach of confidence. It would also be unfair, as a person would not expect their diagnosis of leukaemia to be placed in the public domain and would expect it to remain confidential. But he said that this did not mean that Mr Collie should not have been provided with information. He referred to the fact that, in response to his initial draft decision, the Agency had provided him with a copy of a document entitled *Draft Guidance on Handling Small Numbers*, which was subsequently published by the Information Services Division (ISD) of National Health Services in Scotland in July 2005. It set out a process to be followed when handling statistics where there is a potential risk of disclosure of personal information as a result of small cell counts. This is a disclosure control method, known as "barnardisation". As employed by ISD, it uses a modification rule which adds 0, +1, or –1 to all values where the true value lies in the range from 2 to 4 and adding 0 or +1 to cells where the value is 1. 0s are always kept at 0. It does not guarantee against disclosure but aims to disguise those cells that have been identified as unsafe.

11. In paras 113 and 114 of the decision the Commissioner said that provision of information in this alternative form would provide the closest fit to fulfilling Mr Collie's request, and that the Agency could have offered it to him under its duty to provide advice and assistance under section 15 FOISA. He found that the Agency did not deal with Mr Collie's request for information in accordance with Part I of FOISA 2002 and did not provide him with advice and assistance as to what information it was possible for it to supply to him. He ordered it to provide the census ward data for 1990 to 2001 for the DG postal area in a barnardised form to Mr Collie, unless he would prefer to receive alternative information on aggregate annual figures for the whole Dumfries and Galloway Health Board area.

12. The Agency appealed against this decision to the Court of Session, to which an appeal lies on a point of law under section 56 FOISA against a decision by the Commissioner under section 49 of that Act. The First Division (the Lord President (Hamilton) and Lords Nimmo Smith and Marnoch) refused the appeal. It held that a table setting out the census ward data, barnardised in the manner described by the Commissioner, would not constitute personal data of any of the children resident in the area who had in a relevant year been diagnosed with leukaemia. It was information that was held by the Agency at the time when the request was received, and the Commissioner was entitled to require the Agency to provide this data in the exercise of his supervisory powers under the Act.

13. The issues raised by the appeal against this decision to your Lordships' House require a series of questions to be addressed: (a) was the information which the Commissioner ordered the Agency to release in barnardised form to Mr Collie "held" by the Agency at the time of his request, (b) if it was, would information in this form constitute "personal data", (c) if so, would its release to Mr Collie be in accordance with the data protection principles, (d) in particular, would it meet at least one of the conditions for the processing of personal data in Schedule 2 DPA 1998, (e) if so, would the information also constitute "sensitive personal data", (f) if it would, would its release to Mr Collie also meet at least one of the conditions for processing sensitive personal data in Schedule 3 DPA 1998.

Was the data to be barnardised information "held" by the Agency?

14. The general entitlement of an applicant to receive the requested information from a Scottish public authority applies only to information which is "held" by it at the time the request is received: section 1(4) FOISA 2002. The Agency submits that the process of barnardisation would require the production or making of information that was different from that which was held by it at the time of the request. The process required information to be created, and until this was done it was not "held" by the Agency. The Secretary of State for Justice, in a helpful intervention, has drawn attention to the fact that the question whether an authority holds information which does not actually exist in the form and with the contents requested but which could be created from information which it does unquestionably hold is one which very commonly arises in practice. He submits that the obligations of public authorities ought to be limited to information which is truly held by them so that they are not put into the position of having to conduct research or create new information on behalf of requesters.

15. It seems to me that the position that the Agency has adopted to the request in this case is an unduly strict response to what FOISA requires. This part of the statutory regime should, as Lord Marnoch said, be construed in as liberal a manner as possible. The effect of barnardisation would be to apply a form of disguise, or camouflage, to information that was undoubtedly held by the Agency at the time of the request. It would amount to the provision of that information in a form that concealed those parts of it that have to be withheld but which would nevertheless, to some degree, convey to the recipient information that was undoubtedly held by the Agency at the time of the request. The process is similar to that of redaction, which involves doing something to information in the form in which it was held so that those parts of it which are not private or confidential can be released. It would not amount to the creation of new information, nor would it involve the carrying out of any research. It would be to do no more than was reasonable in the circumstances, having regard to the need for the form in which the information was disclosed to comply with the data protection principles.

16. The latitude which should be given to a request which cannot be met in the form requested is indicated by section 11(2)(b) FOISA which provides for the provision of a digest or summary of the information, and by section 11(4) which provides that information may be given by any means which are reasonable in the circumstances. No hard and fast rules can be laid down as to what it may be reasonable to ask a public authority to do to put the information which it holds into a form which will enable it to be released consistently with the data protection

principles. Protection against the excessive cost of compliance is provided by section 12 FOISA. But it has not been suggested that the process of barnardisation which the Commissioner said should be adopted in this case would be excessively costly. In my opinion information in that form would contain information that was "held" by the Agency at the time of the request and, unless it was "personal data" and its disclosure would contravene any of the data protection principles, it would have to be released in response to it.

Would the barnardised data be "personal data"?

17. One can sympathise with the difficulties which the Commissioner faced when he was asked to deal with this aspect of the case within a very short time of taking up his appointment. But it has to be said, with respect, that the approach which he took to it suffers from a number of defects. Most important of all, he did not ask himself whether the barnardised data would be personal data within the meaning of section 1(1) DPA and, if so, whether its disclosure to Mr Collie would satisfy the disclosure principles. In the result he did not find it necessary to consider whether release of the data in that form would be in accordance with the data protection principles.

18. The Commissioner indicated in para 109 that he regarded the provision of the information in the barnardised form as less disclosive. He said in para 113 that he thought that it would provide the closest fit to fulfilling Mr Collie's request. He treated the provision of the data in that form as an appropriate response by the Agency under section 15 FOISA. That section requires a public authority to provide, so far as it is reasonable to expect it to do so, advice and assistance to a person who has made a request for information. But the effect of the Commissioner's decision was to require the Agency to release information to Mr Collie, not just to give him advice or assistance. He did not pursue the point to its proper conclusion. This was an error of law. Its release would only have been appropriate if he was satisfied that it was not personal data in the hands of the Agency to which the first condition in section 38(2)(a)(i) applied or, if it was, that disclosure of the information in this form would not contravene any of the data protection principles. His decision contains no findings on these points.

19. In the First Division the Lord President looked for guidance as to how to approach the problem to the decision of the Court of Appeal in *Durant v Financial Services Authority* [2003] EWCA Civ 1746; [2004]

FSR 28. That was a case where the person who was seeking disclosure of the information was the data subject, as he was the individual who was the subject of the personal data to which he request related. Part II DPA 1998 contains provisions which are designed, on certain conditions, to enable the data subject to obtain access to such information. Among these provisions are sections 7(4) and section 8(7), which enable the data controller to refuse to disclose the information if the data subject would be able to identify another person from the information which he would have to supply to comply with the request and any other information which, in his reasonable belief, is likely to be in, or come into, the possession of the data subject. It was in that context that Auld LJ said in para 28 that mere mention of the data subject in a document held by a data controller did not necessarily amount to his personal data and suggested two notions that might be of assistance in determining whether it did. One of these was whether the information was biographical in a significant sense. The other was one of focus.

20. The Lord President, applying the second of these two guidelines, said in para 23 that the effect of barnardisation was to move the focus of the information away from the individual children to the incidence of disease in particular wards in particular years. It may indeed have this effect. But this does not resolve the question whether or not it is "personal data" within the meaning of DPA 1998, which is the question that must be addressed in this case. I do not think that the observations in *Durant v Financial Services Authority* on which the Lord President relied have any relevance to this issue. The answer to the problem must be found in the wording of the definition in section 1(1), read in the light of Council Directive 95/46/EC which was adopted on 24 October 1995 and Member States were obliged to implement by 1998.

21. Section 1(1) defines "personal data" in these terms:

> "'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."

The word "data" is also defined in section 1(1), although the word "information" is not. For the purposes of DPA 1998 "data" means information which is in a form capable of being processed by a computer or other automatic equipment, or is recorded with the intent that it be should be processed by such means, or is recorded as part of a relevant filing system, such as a card file, which is structured in such a way that specific information relating to a particular individual is readily accessible or is part of an accessible record as defined by section 68, such as a set of notes kept by a health professional which relate to a named patient. The word "processing" is also given a wide meaning by section 1(1). It includes carrying out any operations on data, including adapting, altering or disclosing it.

22. As the definitions in section 1(1) DPA make clear, disclosure is only one of the ways in which information or data may be processed by the data controller. The duty in section 4(4) is all embracing. He must comply with the data protection principles in relation to all "personal data" with respect to which he is the data controller and to everything that falls within the scope of the word "processing". The primary focus of the definition of that expression is on him and on everything that he does with the information. He cannot exclude personal data from the duty to comply with the data protection principles simply by editing the data so that, if the edited part were to be disclosed to a third party, the third party would not find it possible from that part alone without the assistance of other information to identify a living individual. Paragraph (b) of the definition of "personal data" prevents this. It requires account to be taken of other information which is in, or is likely to come into, the possession of the data controller.

23. The question then is whether the respondent can meet Mr Collie's request by requiring the Agency to release the information to him in a barnardised form. Barnardisation is a method of rendering the information, so far as it is possible to do so, anonymous. If the definition of "personal data" can be read in a way that excludes information that has been rendered fully anonymous in the sense that it is information from which the data subject is no longer identifiable, putting it into that form will take it outside the scope of the Agency's duty as data controller under section 4(4) DPA 1998 to comply with the data protection principles. It will also remove it from the definition of exempt information in section 38 FOISA 2002. This is because that definition extends only to information which is "personal data" within the meaning of section 1(1) DPA 1998. If the definition of "personal data" cannot be read in this way, it will not be open to the respondent to require the Agency to release the information to Mr Collie, even

although barnardised to eliminate any possible risk of identification, unless processing it in this way would be in accordance with the data protection principles. There is an obvious attraction in the first of these two routes towards meeting the request, as it is a much simpler way of dealing with it. But is the definition open to this construction?

24. The relevant part of the definition is head (b). It directs attention to "those data", which in the present context means the information which is to be barnardised, and to "other information" which is or may come to be in the possession of the data controller. "Those data" will be "personal data" if, taken together with the "other information", they enable a living individual to whom the data relate to be identified. The formula which this part of the definition uses indicates that each of these two components must have a contribution to make to the result. Clearly, if the "other information" is incapable of adding anything and "those data" by themselves cannot lead to identification, the definition will not be satisfied. The "other information" will have no part to play in the identification. The same result would seem to follow if "those data" have been put into a form from which the individual or individuals to whom they relate cannot be identified at all, even with the assistance of the other information from which they were derived. In that situation a person who has access to both sets of information will find nothing in "those data" that will enable him to make the identification. It will be the other information only, and not anything in "those data", that will lead him to this result.

25. The wording of recital 26 of the preamble to the Directive supports this approach. It provides:

> "Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable."

The definition of "personal data" gives effect to recital 26. The first phrase in the recital is the situation referred to in head (a) of the definition, where the information itself enables the person to whom it relates to be identified. The second phrase is the situation referred to in head (b), where the information has this effect when taken together with other information. The third phrase casts further light on what Member

States were expected to achieve when implementing the Directive. 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 protection. Read in the light of the Directive, therefore, the definition in section 1(1) DPA 1998 must be taken to permit the release of information which meets this test without having to subject the process to the rigour of the data protection principles.

26. The effect of barnardisation would be to conceal, or disguise, information about the number of incidences of leukaemia among children in each census ward. The question is whether the data controller, or anybody else who was in possession of the barnardised data, would be able to identify the living individual or individuals to whom the data in that form related. If it was impossible for the recipient of the barnardised data to identify those individuals, the information would not constitute "personal data" in his hands. But we are concerned in this case with its status while it is still in the hands of the data controller, as the question is whether it is or is not exempt from the duty of disclosure that FOISA says must be observed by him.

27. In this case it is not disputed that the Agency itself holds the key to identifying the children that the barnardised information would relate to, as it holds or has access to all the statistical information about the incidence of the disease in the Health Board's area from which the barnardised information would be derived. But in my opinion the fact that the Agency has access to this information does not disable it from processing it in such a way, consistently with recital 26 of the Directive, that it becomes data from which a living individual can no longer be identified. If barnardisation can achieve this, the way will be then open for the information to be released in that form because it will no longer be personal data. Whether it can do this is a question of fact for the respondent on which he must make a finding. If he is unable to say that it would in that form be fully anonymised he will then need to consider whether disclosure of this information by the Agency would be in accordance with the data protection principles and in particular would meet any of the conditions in Schedule 2. This is the more difficult of the two routes that I have mentioned. As the issues were fully argued I shall say what I think about them. But there is no doubt that the respondent's task will be greatly simplified if he is able to satisfy himself that the process of barnardisation will enable the data to be sufficiently anonymised.

The data protection principles

28. The respondent's approach, as I understand it and which – if I am right about this – I would respectfully approve, has been to try to use the barnardisation system to take the data out of the "personal data" category. If this proves not to be possible however thought will have to be given to the detailed provisions of the relevant schedules and as to how any of the conditions that they contain might be met so that the information could be released to Mr Collie compatibly with the data protection principles. Neither the Agency nor the Commissioner made any submissions on this point in their written cases. But the Secretary of State did deal with it in his written submissions and the parties were able to address it in oral argument. The conditions require careful treatment in the context of a request for information under FOISA 2002. It must be borne in mind that they were not designed to facilitate the release of information. They were designed for the context in which they appear, which is the protection of personal data from processing in a way that might prejudice the rights and freedoms or legitimate interests of the data subject.

29. Section 4(4) DPA provides that it shall be the duty of the data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller. These principles are the data protection principles set out in Part I of Schedule 1 to the Act. The definition of "processing" in section 1(1) DPA includes the disclosure of information or data by transmission, dissemination or making it available. FOISA 2002 has greatly increased the range of circumstances in which a data controller may be required to process information in this way, but section 38(2)(b) FOISA 2002 insists that this may only be done in compliance with the data protection principles. The first principle begins by stating that personal data shall be processed fairly and lawfully. That was the test that was applied by the Commissioner to the unbarnardised information in paras 101 to 105 of his decision. But the principle goes on to state "in particular" that personal data shall not be processed unless at least one of the conditions in Schedule 2 for the processing of personal data and of Schedule 3 for the processing of sensitive personal data is met.

30. The Commissioner said in paras 101 to 105 of his decision, after concluding that the unbarnardised data at census ward level was personal data as defined by section 1(1) DPA 1998, that its disclosure

would breach the first data protection principle because disclosure would be unfair and unlawful. He did not express any view as to whether any of the conditions in Schedule 2 for the processing of personal data were met. Nor did he express any view as to whether the information was "sensitive personal data" within the meaning of section 1(1) DPA and, if so, whether any of the conditions in Schedule 3 for the processing of such data were also met. The concept of fairness for the purposes of the first data protection principle is explained in Part II of Schedule 1. It is concerned essentially with the method by which the information is obtained, and in particular with whether the person from whom it was obtained was deceived or misled. In this case the processing which is in issue is the disclosure of statistical information in the possession of the Agency, and there is no suggestion that any unfairness of that kind will be involved. The concept of lawfulness cannot sensibly be addressed without considering the conditions set out in Schedule 2 and in Schedule 3 also, if it is applicable, because any disclosure which fails to meet at least one of the conditions in these Schedules would be contrary to section 4(4) DPA 1998. This is made clear by the words "in particular" in the first principle.

The Schedule 2 conditions

31. Schedule 2 DPA 1998 sets out six conditions which are relevant for the processing of any personal data. At least one of these conditions must be met if the data controller is to comply with section 4(4) of the Act, which requires him to comply with the data protection principles in relation to all personal data of which he is the data controller. Mr Cullen submitted that the condition in Schedule 2 that is relevant to this case is para 6(1), which provides:

> "The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject."

Condition 5(b) may also be relevant. It provides:

> "The processing is necessary –
> …

(b) for the exercise of any functions conferred on any person by or under any enactment."

Condition 5(b) reappears in condition 7(1)(b) of Schedule 3 which I will consider in more detail later. The issues which it raised in relation to the dissemination of epidemiological data under para 3(j) of the National Health Service (Functions of the Common Services Agency) (Scotland) Order 1974 are essentially the same as those raised by condition 6.

32. There is no doubt that Mr Collie, and the MSP for whom he was acting, had a legitimate interest in obtaining the information that he requested due to the proximity of the sites at Drundennan, Chapelcross and Sellafield to the census wards in Dumfries and Galloway, and that to enable him to pursue those interests the disclosure of the information was necessary. Mrs Stacey QC for the Agency readily acknowledged that this was so. The question whether its disclosure would prejudice the rights and interests of the children because their identities might be discovered as a result of its release and whether, if so, its release would for this reason be unwarranted is a different matter. Striking the right balance between these two considerations would raise issues of fact as to which no findings have been made and which only the Commissioner is in a position to determine. Resolution of this issue would require the case to be remitted to the Commissioner so that he can carry out this exercise. But if the result of barnadisation is effectively to anonymise the data, no private interests of the children will be affected and there will be no balance to be struck.

33. Then there is the question whether, to comply with section 4(4) DPA 1998, it is necessary for at least one of the conditions in Schedule 3 to be met also. This in turn raises the question whether the information which the barnardised data would contain would constitute "sensitive personal data". As already noted, this was an issue which neither the Commissioner nor the First Division of the Court of Session found it necessary to consider.

Would barnardised data be "sensitive personal data"?

34. Section 2 DPA 1998 provides:

"In this Act 'sensitive personal data' means 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, or

(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."

35. The item on this list which is relevant to this case is item (e). The information which Mr Collie asked for was details of all incidents of childhood leukaemia for all the DG postal area by census ward. This was information about the physical health or condition of the children who had been diagnosed as having this disease. For the reasons already given, I consider that it is open to the Commissioner to hold that the barnardised data would constitute personal data within the meaning which has been given to that expression by section 1(1) DPA 1998. It would seem to be a short step to conclude, that if it was personal data, it must be sensitive personal data too because it was data about the physical health of living children who could be identified from data released in response to the request together with other information in the possession of, or likely to come into the possession of, the Agency. This too is a question of fact on which the Commissioner must make a finding.

36. But Mr Cullen QC for the Commissioner submitted that it would not be open to him because the definition in section 2 was a self-standing definition. The only data that were relevant to the question whether the information was sensitive personal data were the data that were to be processed by releasing it. As it would not be possible from the barnardised data alone to discover the children's identities it could not be said to consist, in that form, of information about their physical health or condition. The difficulty of meeting any of the conditions in Schedule 3 if it was to be released was another factor to be taken into account. A narrow interpretation of the expression was necessary in these circumstances. Otherwise it would not be lawful for information about a matter which was of genuine public interest to be released in this case.

37. I do not think that the wording of the Act as whole supports this interpretation. The fact that the expression that is being defined in section 2 DPA 1998 includes the words "personal data" suggests that the whole of the definition of "personal data" is written into it. This is not just "data" as defined in section 1(1). "Sensitive personal data" is a subset, or a species, of "personal data". This approach is reinforced by section 4(4), which provides:

> "Subject to section 27(1) [exemptions], it shall be the duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller."

The expression "personal data" in this subsection must be taken to mean personal data as defined in section 1(1). The context shows that it is being used here to embrace not only all "personal data" as so defined but also "sensitive personal data", although sensitive personal data as such are not separately identified. This is because the data protection principles make special provision in Schedule 3 for the processing of sensitive personal data. The expression "personal data" must include sensitive personal data to bring that species of data too within the scope of the obligation that is imposed on the data controller by section 4(4).

38. The same use of language is to be found in para 1 of Schedule 1. It sets out the first principle for the processing of "personal data", within which special provision is made for the processing of "sensitive personal data." I can find nothing in the context of this Schedule or of Schedule 3 to suggest that the reference to data of that kind should be read as narrowly as Mr Cullen suggested. The words "personal data" are also used repeatedly in Schedule 3. There seems to me to be no good reason for refusing to apply the full definition of that expression in section 1(1) to its use in this context, especially in view of the way the obligation that section 4(4) sets out is expressed.

39. Reference was made to article 8(1) of the Directive which uses the words "personal data" when it refers in the first place to the processing of data "revealing" some things such as racial and ethnic origin and the word "data" only when it refers in the second place to the processing of data "concerning" health or sex life. But the Directive is not as precise as the statute is in its choice of language, and I would not attach any significance to this aspect of the article. On the contrary, recital 2 read together with article 1(1) of the Directive seem to me to support the view that data of such a sensitive nature as that relating to a

person's health or sex life should be given just as much protection in the hands of the data controller as that relating to his racial or ethnic origin and the other things referred to in the first place in article 8(1).

40. For these reasons I would hold that DPA 1998 requires the definition of "personal data" to be read into the definition of "sensitive personal data". I would not be deterred by any difficulty that may be found in any particular case in meeting any of the conditions in Schedule 3. This is not an appropriate context for the statutory language to be construed liberally in favour of the release of information. DPA 1998, as its short title indicates, is designed to regulate and control the processing of data and to protect the interests of those who may be affected by its release. The definition of "sensitive personal data" forms an essential part of the statutory scheme of data protection. The fact that the definition is relevant to the question whether the data is exempt information as defined by section 38 FOISA 2002 does not justify giving it a narrower meaning than it has for the purposes of DPA 1998. If none of the conditions in Schedule 3 can be met, so be it. This must be taken to be what Parliament intended when the legislation that it enacted was put into effect.

The Schedule 3 conditions

41. Schedule 3 DPA 1998 sets out ten conditions which are relevant for the processing of sensitive personal data. At least one of these conditions must also be met if the data controller is to comply with section 4(4) DPA 1998. Mr Cullen QC was unable to point to any of the conditions on this list which were relevant to this case, except possibly condition 10 which refers to personal data processed in circumstances specified in an order made by the Secretary of State for the purposes of that paragraph. But the circumstances referred to here are those specified in the Data Protection (Processing of Sensitive Personal Data) Order 2000 (SI 2000/417). Mr Cullen did not suggest than any of them applied to this case and, apart possibly from para 9 which deals with processing which is in the substantial public interest, I have not been able to find any that do. The Secretary of State, on the other hand, submitted in his written case that a possible candidate in Schedule 3 was condition 7(1)(b), which is in almost exactly the same terms as condition 5(b) in Schedule 2. It provides:

> "The processing is necessary –

…

(b) for the exercise of any functions conferred on any person by or under an enactment."

42. The National Health Service (Functions of the Common Services Agency) (Scotland) Order 1974, pursuant to which the Agency was established, deals with the release of information which it holds in para 3. It provides:

"It shall be the duty of the Agency to undertake the following functions:

…

(c) the provision of information, advisory, and management services in support of the functions of the Secretary of State and Health Boards other than where the Health Protection Agency is exercising functions under the Health Protection Agency (Scottish Health Functions) Order 2006

…

(j) the collection and dissemination of epidemiological data and participation in epidemiological investigations."

The disclosure of the information to Mr Collie would not fall within head (c) of para 3, which deals with the provision of information in support of the functions of the Secretary of State and Health Boards. But it is arguable that it would fall within head (j) of the paragraph. The question is whether its disclosure to Mr Collie can be said to be "necessary" for the performance of that function, as condition 7(1)(b) of schedule 3 requires. This is a question of fact which only the Commissioner is in a position to determine, as is the further question which is inherent in the opening words of the first data protection principle. That is whether its disclosure would prejudice the rights and freedoms and legitimate interests of the children in the relevant census wards. The case would have to be remitted to him if these issues are to be resolved, as there are no findings in his decision would enable them to be answered by your Lordships.

43. In my opinion it must follow, if the Commissioner finds that the information is sensitive personal data and that none of the conditions in Schedule 3 are met, that it will not be possible for the data at ward census level to be released without contravening the first data protection principle. The Agency, as the data controller, is prohibited by section

4(4) DPA 1998 from processing the data which it holds in a way that does not comply with those principles. That prohibition is built into FOISA 2002 by section 38(1)(b) read together with section 38(2)(a)(i). As this would mean that disclosure of the information would contravene the first data protection principle, it would be exempt information and the Agency would not be under any duty in terms of section 1(1) FOISA to release it to Mr Collie.

Conclusion

44. For these reasons, I am of the opinion that the proper course would be for Mr Collie's application to be remitted to the Commissioner so that he can examine the facts in the light of your Lordships' judgment and determine whether the information can be sufficiently anonymised for it not to be "personal data". If he decides that it cannot be so anonymised, he will need then to consider whether its disclosure to Mr Collie will comply with the data protection principles. In order to satisfy the first of the data protection principles listed in Schedule 1 he will need to decide whether information in that form would also be "sensitive personal data", so that at least one of the conditions in Schedule 3 DPA must be met as well as at least one of the conditions in Schedule 2.

45. I would allow the appeal. I would recall the Court of Session's interlocutor of 1 December 2006 and set aside the decision that the respondent made on 15 August 2005 under section 49(3)(b) FOISA 2002. I would remit Mr Collie's application to him so that he can consider it afresh in the light of the opinions of your Lordships.

LORD RODGER OF EARLSFERRY

My Lords,

46. This appeal arises out of a request by Mr Michael Collie to the Common Services Agency ("the Agency") under the Freedom of Information (Scotland) Act 2002 ("the 2002 Act") to provide the details, by census wards, of all incidents of leukaemia for both sexes, in the age range 0-14, by year, from 1990 to 2003, for all of the Dumfries and Galloway postal area.

47. The Agency was constituted by section 19(1) of the National Health Service (Scotland) Act 1972, which was re-enacted as section 10(1) of the National Health Service (Scotland) Act 1978. The Agency is a "public authority" in terms of section 1(1) of the Data Protection Act 1998 ("the 1998 Act") as amended by article 2 of the Freedom of Information (Scotland) Act 2002 (Consequential Modifications) Order 2004 (SI 2004/3089 (S 10)), since it is listed as one of the Scottish public authorities in Part 4, para 26, of Schedule 1 to the 2002 Act. This has a bearing on the way that the provisions of the 1998 Act apply to the situation.

48. Section 10(1) of the 1978 Act provides that the Agency is to have the functions conferred on it by section 10; subsection (3) gives the Scottish Ministers the power to delegate to the Agency such of their functions under the Act as they consider appropriate. That power was first exercised by the Secretary of State in The National Health Service (Functions of the Common Services Agency)(Scotland) Order 1974 (SI 1974/467). Article 3(j) provides that it shall be the duty of the Agency to undertake "the collection and dissemination of epidemiological data and participation in epidemiological investigations." While some other functions of the Agency have come and gone over the years, this duty has remained throughout.

49. In performance of this duty, the Agency has amassed a vast body of data on a variety of diseases, including cancer and, more particularly, childhood cancers. Nowadays, many of the data are held in a computerised form by the Information Services Division ("ISD") of the Agency. The Scottish Executive uses the information gathered by ISD in administering health services in Scotland. In addition, ISD not only responds to requests from researchers and others for data but regularly publishes statistics derived from its data.

Barnardisation

50. Plainly, a body like the Agency has information about the health of people all over Scotland. Bodies which gather and disseminate such personal information are very conscious of the need to ensure that, when they disclose any of this information, or data derived from the information, the disclosure is done in such a way as to minimise the risk that the individuals to whom the information or data relate can be

identified and, as a result, suffer distress and embarrassment - or worse. Obviously, the risk is greatest where the data are broken down by reference to small units, such as census wards, in which the data will consist of small numbers. Bodies which publish frequency statistics have accordingly developed various techniques - such as combining data for a larger age range or for a larger geographical area, and suppressing particular figures in tables - to counteract the problem. One technique, which is of particular relevance to this appeal, is "barnardisation". It is applied to frequency tables, such as were requested by Mr Collie. The procedure involves modifying each internal cell of every table by +1, 0 or -1. But the technique does not always provide adequate protection, since, when the probability of the event occurring is small, the majority of cells are not modified and so the probability that a 1 is a true 1 is quite high. In such cases the risk of identification may remain unacceptably high.

51. In July 2005 ISD published draft guidance on disclosure control, relating to handling small numbers. It described the goal as being:

> "to devise a method for publishing data that minimises the risk and potential damage to an individual due to inadvertent disclosure of a detail; and to do so without adopting such restrictions that unjustifiably curtail the presentation of information that would otherwise be beneficial to the community at large."

The guidance went on to identify data of a sensitive nature - for example, where there had been a high degree of controversy or stigma in the recent past regarding the subject matter. These included data on sexually transmitted diseases, abortions, mental health diagnoses and alcohol misuse. The guidance went on to explain that ISD employed barnardisation as its preferred method of perturbing data. It also indicated that other techniques for avoiding the risk of individuals being identified - such as grouping by broader age bands, by a larger geographical area, or using aggregated years of data - should be considered. The guidance concluded:

> "Whilst this is straightforward for publications, for customer requests re-specification should only be performed after discussion with the customer to ensure it will continue to meet their needs and this is not wasted effort."

52. Barnardisation is, accordingly, one method of reducing the risk of identification. It does not guarantee that the risk will be eliminated. ISD recognises this, of course. For instance, in its Decision Flow Chart for Handling Small Numbers, it deals with data for a population of <40. Where the numerator, ie, the count in the cell relating to that population, is <5, then, if the data are "sensitive" in terms of the ISD classification – relating, for instance, to a sexually transmissible disease – the data are not to be published. If they are not "sensitive" in that sense, then they are to be barnardised. The difference in treatment shows that ISD recognises that barnardisation will reduce the risk of identification to a level which will be acceptable for some data but not for others. Mrs Stacey QC, who appeared for the Agency, indicated that the ISD draft guidance had subsequently been modified, but the House was not given any details of the modifications.

The Data Protection Act 1998

53. Parliament first sought to regulate bodies which used data relating to individuals in the Data Protection Act 1984, but that Act was repealed and replaced by the 1998 Act. According to the long title, the purpose of the 1998 Act was "to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information." All the operations mentioned in the long title, and others besides, are lumped together as aspects of the "processing" of data: section 1(1) of the 1998 Act. References to "disclosing" in relation to personal data include "disclosing the information contained in the data": section 1(2)(b).

54. Counsel who drafted the 1998 Act was careful to distinguish between "information" and "data". The 2002 Act maintains that distinction. See, for instance, section 38(1) of that Act. In section 1(1) of the 1998 Act as amended by section 68(2) of the Freedom of Information Act 2000 ("the 2000 Act"), the term "data" is defined widely:

> "'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,
(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68; or
(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d)…."

According to paragraphs (a) and (b) of this definition, data include information being processed by a computer, or being recorded with the intention that it should be processed in that way. The term also covers information recorded as part of a relevant filing system (para (c)) and information, not falling within paras (a)-(c), forming part of a health record (para (d) and section 68(1)(a)). Finally, by virtue of para (e), it covers recorded information held by a public authority which does not already fall within any of paragraphs (a) to (d). Para (e) was inserted at the time when the Freedom of Information legislation was brought into effect in order to ensure that, subject to any specified restriction, both the United Kingdom and Scottish Acts covered all the recorded information held by a public authority. Since the Agency is a public authority, in the present case, in effect, any recorded information held by the Agency constitutes "data" held by it for the purposes of the 1998 Act.

55. The data controller is the person who determines the purposes for which, and the manner in which, any personal data are, or are to be, processed: section 1(1). So there is no doubt that ISD is the data controller for any centrally held epidemiological data on human health in Scotland which fall within the definition of "personal data".

56. In so far as the information being processed relates to individuals who are no longer alive, it simply constitutes "data" in terms of section 1(1)(a). But, in so far as it relates to living individuals, the information may fall within the narrower category of "personal data". That term is defined, again in section 1(1), as meaning:

"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 likely to come into the possession of, the data controller…."

An individual who is the subject of personal data is a "data subject". But, in fact, if "personal data" consist of information as to the data subject's physical or mental health or condition, they fall within a particular subset of personal data, viz "sensitive personal data": section 2. That subset includes data consisting of information about other sensitive matters, such as the data subject's political opinions, religious beliefs and sexual life. The classification matters because the regulation of the processing of sensitive personal data is, understandably, tighter than the regulation of the processing of other personal data. In practice – as I noted previously - ISD treats personal data relating to certain medical conditions, such as mental health conditions and sexually transmissible diseases, as being more sensitive than data relating to other medical conditions because of the stigma which may attach to them and cause embarrassment to the data subject.

57. Section 4(4) of the 1998 Act regulates the processing of personal data - and only personal data - by the data controller by imposing on him a duty to comply with the data protection principles. This duty is intended to ensure that those with access to data relating to individuals cannot retrieve them except for proper purposes. The principles themselves are found in Schedule 1 to the 1998 Act. The principle which matters for present purposes is the first, which is set out in para 1 of Part I of the schedule:

"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."

As is apparent, no personal data are to be processed unless one of the conditions in Schedule 2 is met. But, in the case of sensitive personal data, they are not to be processed, unless, in addition, at least one of the conditions in Schedule 3 is met. It is, partly at least, by insisting that this second hurdle must be overcome before sensitive personal data can be processed that the 1998 Act achieves the tighter regulation of the processing of personal data consisting of information as to the data subject's health. Even if the conditions in Schedules 2 and 3 are met, however, the data controller cannot process the data if it would not be fair or lawful to do so.

58. It follows that, under the 1998 Act, no-one in ISD can process – for example, by accessing or disclosing - personal data consisting of information as to an identifiable individual's health, unless at least one of the conditions in each of Schedules 2 and 3 is met.

59. So far as Schedule 2 is concerned, it seems clear that ISD needs to process personal data for the exercise of the functions - collecting and disseminating epidemiological data and participating in epidemiological investigations - conferred on it by the then Secretary of State under the predecessor to section 10(3) of the 1978 Act. So, prima facie, condition 5(b) would apply. Condition 6(1) also appears to be potentially relevant to the issue in these proceedings, since it deals specifically with the disclosure of personal data. It provides:

> "The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject."

60. Assuming that any disclosure of sensitive personal data might satisfy one or other of these conditions, it could still not take place unless it met one or more of the conditions in Schedule 3. But, not surprisingly, para 7(1)(b) of Schedule 3 is in precisely the same terms as para 5(1)(b) of Schedule 2. So, if the processing of the data would prima facie meet the condition in para 5(1)(b) of Schedule 2, it would also prima facie meet the condition in para 7(1)(b) of Schedule 3.

61. There is no other condition in Schedule 3 as enacted which would seem to be potentially relevant, but para 9 of the Schedule to the Data Protection (Processing of Sensitive Personal Data) Order 2000 (SI 2000/417) specifies the following circumstances in which data are to be processed:

> "The processing—
>
> (a) is in the substantial public interest;

(b) is necessary for research purposes (which expression shall have the same meaning as in section 33 of the Act);
(c) does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of that data subject; and
(d) does not cause, nor is likely to cause, substantial damage or substantial distress to the data subject or any other person."

It is at least conceivable that, depending on the circumstances, this condition might be of relevance – but I express no view on the point which was not fully argued.

62. Assuming that processing the sensitive personal data would meet at least one of the conditions in each of Schedules 2 and 3, ISD would still only be able to disclose them if it would be fair and lawful to do so.

The Freedom of Information (Scotland) Act 2002

63. My Lords, I have so far been outlining the system of regulation which, apart from para (e) of the definition of "data", applied to the Agency's operations of obtaining, storing and disclosing sensitive personal data under the 1998 Act before the 2002 Act was brought into force. It is important to realise that all these provisions remain in full force and effect. When the Scottish Parliament came to enact the 2002 Act, in order to give people a right to information from Scottish public authorities, it did not destroy, but built upon, the system created by the 1998 Act. Indeed, it had no power to amend the 1998 Act, which relates to a reserved matter. Basically, therefore, the Scottish Parliament wanted to maintain the high degree of protection afforded by the 1998 Act to individuals whose data were processed by Scottish public authorities, and, yet, to give third parties an effective right to obtain information from those public authorities. So the system of regulation of data processing under the 1998 Act remains in place, but the Parliament has grafted on to it provisions for third parties to obtain information without the operation of the pre-existing system of protection for data subjects being compromised. It has not been suggested in this case that the legislation is incompatible with any Convention right.

64. The key provisions in the 2002 Act come at the very start. Section 1(1) provides:

> "A person who requests information from a Scottish public authority which holds it is entitled to be given it by the authority."

I have already pointed out that the Common Services Agency is a Scottish public authority in terms of Part 4, para 26, of Schedule 1 to the Act.

65. By section 1(6), a person has no right to information, however, if it is exempt information in terms of section 2 of the 2002 Act. Among the varieties of exempt information is information which constitutes "personal data" and whose disclosure to a member of the public, otherwise than under the Act, would contravene the data protection principles in the 1998 Act: sections 2(1) and (2)(e) and 38(1)(b) and (2)(a)(i) and (b) of the 2002 Act.

66. Section 38(1) provides inter alia:

> "(1) Information is exempt information if it constitutes -
> (b) personal data and either the condition mentioned in subsection (2) (the 'first condition') or that mentioned in subsection (3) (the 'second condition') is satisfied;
> ...
> (2) 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 (c. 29), 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….
> …
> (b) in any other case, that such disclosure would contravene any of the data protection , that such disclosure would contravene any of the data protection principles if the exemptions in section 33A(1) of that Act (which relate to manual data held) were disregarded."

All the information held by the Agency must fall within either paras (a) to (d) or para (e) of the definition of data in section 1(1) of the 1998 Act. So either para (a) or para (b) of section 38(2) is in play in respect of all the personal data held by the Agency. In practice, in this case, the distinction does not matter. Subsection (5) gives the expressions "the data protection principles", "data subject" and "personal data" the same meanings as in Schedule 1, to and section 1(1) of, the 1998 Act. Since there is no mention of "sensitive personal data", the Parliament must simply have treated such data as being caught by any references to "personal data".

67. Information will therefore be exempt from disclosure if (1) it constitutes personal data and (2) the disclosure of the information to a member of the public, otherwise than under the 2002 Act, would contravene the data protection principles in Schedule 1 to the 1998 Act. In particular, therefore, personal data will be exempt from disclosure under the 2002 Act if their disclosure to a member of the public would contravene the first data protection principle. And their disclosure will indeed contravene that principle if it is unfair or unlawful. Moreover, it will contravene that principle unless at least one of the conditions in Schedule 2 to the 1998 Act is met and, in the case of sensitive personal data, unless one of the conditions in Schedule 3 to that Act is also met. In other words, the same safeguards against the disclosure of personal data and sensitive personal data as applied before the enactment of the 2002 Act continue to apply today. That is the scheme settled by the legislature.

68. Where the legislature has thus worked out the way that the requirements of data protection and freedom of information are to be reconciled, the role of the courts is just to apply the compromise to be found in the legislation. The 2002 Act gives people, other than the data subject, a right to information in certain circumstances and subject to certain exemptions. Discretion does not enter into it. There is, however, no reason why courts should favour the right to freedom of information over the rights of data subjects. If Lord Marnoch's observations, 2007 SC 231, 241-242, para 32, were intended to suggest otherwise, I would respectfully disagree.

The Present Case

69. As I indicated at the outset, shortly after the 2002 Act came into force, Mr Collie made a request on behalf of a Green Party MSP for the

Agency to provide him with the details, by census wards, of all incidents of leukaemia for both sexes, in the age range 0-14, by year, from 1990 to 2003 for all of the Dumfries and Galloway postal area. Eight days later, the Agency confirmed that it held the data for the period up until 2001 and that it had looked at the data by census ward. But the Agency declined to supply the information since it took the view that, because of the small number of cases in each ward, there was a significant risk of indirect identification of living individuals. For that reason, the Agency considered that the information which had been requested was likely to constitute "personal data" as defined in section 1(1) of the 1998 Act. That being so, it considered that the data constituted exempt information which Mr Collie was not entitled to be given in terms of sections 1(1) and (6) and 2 of the 2002 Act.

70. Mr Collie appealed to the Scottish Information Commissioner ("the Commissioner"), who is the respondent in this appeal. The Commissioner was satisfied that the information sought by Mr Collie was indeed personal data and that disclosing it in its entirety would entail a breach of the first data protection principle in para 1 of Schedule 1 to the 1998 Act, because its disclosure would be unfair and unlawful.

71. But the Commissioner went on to hold that the Agency had been in breach of its duty under section 15 of the 2002 Act to provide Mr Collie with advice and assistance. In particular, the Agency had failed to provide Mr Collie with information as to the wards in which there had been no cases of leukaemia. Secondly, the Agency had been under a duty to consider whether information could have been provided to Mr Collie in a "less disclosive" manner by perturbing the data so that the risk of personal identification would be "substantially removed" and telling Mr Collie what had been done and why. The Commissioner accordingly required the Agency to provide the census ward data for the relevant years in a barnardised form.

72. The Agency appealed to the Court of Session, but the First Division (the Lord President, Lord Nimmo Smith and Lord Marnoch) refused the appeal: 2007 SC 231. The Agency appeals to this House against that decision.

Was the information requested by Mr Collie "personal data"?

73. The disposal of Mr Collie's request depends, in the first place, on whether the information which he sought constitutes "personal data" as defined in section 1(1) of the 1998 Act. If it does not, then nothing in section 2 of the 2002 Act would take it outside the scope of Mr Collie's entitlement under section 1(1) of that Act. But, secondly, even if the information does constitute "personal data", the Agency will still be obliged to supply it, if that can be done without contravening the data protection principles in Schedule 1 to the 1998 Act. And, if supplying the information in one form would contravene those principles, in my opinion, section 1(1) of the 2002 Act obliged ISD to consider whether it could comply with its duty by giving the information in another form. Relevant factors would, of course, include the time allowed by section 10 for complying with requests and any expenditure limit prescribed under section 12.

74. The information which Mr Collie requested was about the incidents of childhood leukaemia in both sexes, by year, in census wards in the Dumfries and Galloway area. As the definition of "sensitive personal data" in section 2 shows, information about a living individual's medical condition will undoubtedly constitute "personal data" if the other requirements of the definition are satisfied. So there is no need in this case to consider the kinds of issue which the Court of Appeal addressed in *Durant v Financial Services Authority* [2004] FSR 28. Everything I go on to say about personal data proceeds on the assumption that the only element in question is the identification of the individual to whom the data relate.

75. It is common ground that ISD itself can identify the individuals to whom the data requested by Mr Collie relate. At the hearing, the argument was that, in these circumstances, the data constituted "personal data" because, in terms of paragraph (b) of the relevant definition in section 1(1) of the 1998 Act, the individuals could be identified either from the data themselves or from the data and other information in the possession of ISD. For instance, even if the data were held in an anonymised form, ISD would also hold the key ("other information") that would allow it to identify the individuals to whom the data related. My noble and learned friend, Lord Hope of Craighead, has proceeded on the basis of paragraph (b). I would agree with his approach, if paragraph (b) does indeed apply.

76. On reflection, however, I consider that paragraph (b) is not relevant in this case. As already observed, Parliamentary counsel was careful to distinguish between "information" and "data". In the present

case, the effect of the inclusion of para (e) in the definition of "data" in section 1(1) of the 1998 Act is that all the recorded information about an individual held by the Agency must fall within the definition of "data". So, if one asks what data the Agency holds on an individual, it is all the information which it has relating to that individual. If the individual to whom all the information relates is identifiable from some information in the data, then all the data count as "personal data". Suppose, for instance, that the Agency holds various pieces of information about a living individual, identified in each case by a different code number. The Agency also holds other items of information in the shape of the various keys to unlock the different code numbers and identify the individual to whom the pieces of information relate. In that situation, all the items of information relating to the individual identified by the code number and the keys themselves are "data" and those data relate to an individual who can be identified from them. So they are all "personal data" in terms of para (a) of the definition: all the data relate to an individual who can be identified from those data. The processing of any of those data is the processing of personal data.

77. Paragraph (b) of the definition of "personal data" applies in a different situation. It applies where the individual to whom data relate is identifiable not from the data themselves but from "other information", ie information which does not count as "data" because it does not fall under any of paras (a) – (e) in the definition of data. So it applies where a public authority does not yet hold information but is likely to come into possession of the information (which will then count as "data") - and that information will make it possible to identify a living individual to whom existing data relate. It also applies where the data controller, who is not a public authority, possesses relevant information which does not, however, fall within any of paras (a) – (d) of the definition of "data" in section 1(1) of the 1998 Act. That could include, for instance, a single sheet of paper containing the key which identified the individual to whom data, as defined in paras (a) to (d) of the definition, related. The data would be "personal data" if the person to whom they related could be identified from the "information" on that sheet of paper.

78. It follows that, in the present case, the question is simply whether, in terms of para (a) of the definition, the data which ISD has been asked to disclose are "personal data" because they "relate to a living individual who can be identified – (a) from those data…."

79. There is nothing in the papers to indicate what actual steps would have been involved in preparing any information or data to be supplied

by the Agency in response to the request by Mr Collie. It is at least possible that, in order to produce the relevant information, ISD would have had to access medical records relating to individuals whom it could identify, whether by using a separate key or otherwise. If so, that step would unquestionably have involved the processing of personal data, to which the data protection principles would have applied. But would the resulting data still constitute "personal data" when they were extracted and put into the relevant tables ready for disclosure? The data would undoubtedly relate to living individuals, but could those individuals be identified from those data? That is a question of fact. If the individuals could be identified, the data would be "personal data"; if they could not be identified, the data would just be – to adopt a description used by Lord Hoffmann in a completely different context - "plain vanilla" data.

80. Assume, for instance, that a data controller, who can indeed identify the individuals to whom all the data relate, aggregates the sensitive personal data for such a large geographical area that it becomes impossible for anyone else to identify the individuals in question from the aggregate data. The data remain "personal data" in the data controller's hands for so long as, by using reasonable means, he can still identify the individuals to whom they relate. He accordingly, remains subject to regulation by the 1998 Act if he processes those data - even by simply holding or retrieving them.

81. But, suppose the data controller takes further steps, say, by removing any identifying codes and separating off the data comprising the aggregate totals for the large geographical area, so that it is then impossible for him to make any connexion between the aggregate data and the individuals concerned. In that situation, the individuals to whom the aggregate data related could no longer be identified from the aggregate data. So the aggregate data would not constitute "personal data", but plain vanilla data. The processing of plain vanilla data is not regulated by the 1998 Act. Moreover, if the plain vanilla data are held by a Scottish public authority, the exemption in section 2 of the 2002 Act does not apply.

82. This result is consistent with the spirit of Council Directive 95/46/EC which the 1998 Act is intended to implement. In particular, recital 26 to the directive presupposes that "the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable…."

83. It follows, that, if ISD could have complied with Mr Collie's request by supplying him with fully anonymised data from which it would have been impossible to identify the individuals to whom the figures related, then the data would not have constituted "personal data" and so the exemption under sections 1(6) and 2 of the 2002 Act would not have applied. That might well have been the case, for example, if Mr Collie had been content with ISD's offer to supply the aggregate figures for the whole Dumfries and Galloway Health Board Area for the entire period from 1990 to 2001. But, by appealing to the Commissioner, he indicated that this offer was not acceptable.

84. The Commissioner readily concluded that the data in the form sought by Mr Collie would constitute "personal data" because, due to the small counts in the cells, the individuals to whom the data related could have been identified by members of the public. The Commissioner went on to hold that disclosure of the data in that form would be unfair and unlawful and would, accordingly, contravene the first non-disclosure principle.

85. The Commissioner held, however, that the Agency should, at least, have disclosed the cells which contained zero, since those cells did not contain personal data. Although perhaps at first sight attractive, that argument must be rejected since, inevitably, by publishing the cells with zeros, ISD would have identified those other cells which contained a count for any year. And, given the small counts and the small areas involved, this would have created very much the same risk of individuals being identified as publishing the counts of 1 or more for the other cells.

86. Although the Commissioner was satisfied that ISD had good reason not to supply the actual positive counts, he ordered the Agency to supply Mr Collie with the information which he sought in a different, barnardised, form, if (as was the case) he did not prefer to receive the aggregate figures. The First Division held that such barnardised data would no longer have constituted "personal data" in terms of section 1(1) of the 1998 Act. Counsel for the Commissioner supported that view. He argued that, if the data are barnardised, so that anyone from outside the Agency sees only the data with random adjustments, they no longer relate to any particular individual and so have ceased to be "personal data" for purposes of section 1(1) of the 1998 Act. The First Division accepted that argument. I would reject it.

87. The question only arises, of course, if, immediately before they are barnardised, the data are indeed personal data, because the individuals to whom they relate can be identified from them. When the

data are barnardised, statistical noise is introduced into the tables, but the tables contain no new information: the counts in the cells still relate to the same diagnoses. For instance, if there is one girl diagnosed with leukaemia in a particular census ward in a particular year, the barnardised data for that ward will still relate to the fact that that girl was diagnosed as suffering from leukaemia in that year: the only difference is that, randomly, the count relating to that girl may now be 1 or 2. Barnardising is simply one method which can be used by those publishing frequency tables to minimise the risk of revealing the identities of the individuals to whom the counts relate. If, however, even after barnardisation, the individuals to whom the data relate can still be identified, the data remain "personal data". Whether or not the individuals are identifiable from the barnardised data is a question of fact, the answer to which may vary from situation to situation and, indeed, from individual to individual.

88. In this case, the Commissioner did not actually hold that barnardising the data would have made it impossible to identify the individuals to whom they related. Rather, he held that it would have substantially removed the risk of them being identified. In my view, however, the material which the Agency placed before the Commissioner did not provide an adequate basis for that conclusion. Indeed, at first sight, it seems at least possible that, with the very small counts in the cells in the tables, the individuals in question could still be identified from those data. Counsel for the Commissioner accepted that, if the supposed factual basis for his decision were flawed in this way, it would be appropriate for the decision to be quashed and for him to reconsider it.

Disposal

89. For these reasons I would allow the appeal and make the order proposed by my noble and learned friend, Lord Hope of Craighead.

BARONESS HALE OF RICHMOND

My Lords,

90. Mr Collie asked the Common Services Agency for the incidences of childhood leukaemia in the age range 0 to 14 in each year from 1990

to 2003 and for each census ward in the Dumfries and Galloway postal area. The Commissioner held that he could not have the information in that form, because of the risk that recipients might be able to identify individuals from it. But he also held that it should be provided "suitably amended to protect against potential identification of individuals". There is some reason to think that, even amended in the way which he had in mind ("barnardised"), there would still be a risk that individuals could be identified. But that is a question of fact for the Commissioner.

91. We can easily understand the public interest in making this information available. If I were a parent living in the area I would certainly want to know. We would all like the legal position to be that, if the risk of identification can indeed be eliminated, the Agency is obliged to provide it. That reflects the expectation in Recital 26 of the European Directive 95/46/EC: that the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable. It would have been so much easier if this had been clearly stated in the Data Protection Act 1998.

92. Much though I would like that to be the position, I have had much more difficulty in spelling it out from the definition of "personal data" in section 1(1) of the Act. In the end, however, I have reached it by the following route. For this purpose, I am assuming the particular data which Mr Collie has requested, anonymised in such a way that neither he nor anyone else to whom he might pass them on could identify the individuals to whom they relate. The Agency may well have the key which links those data back to the individual patients. The Agency therefore could identify them and remains bound by the data protection principles when processing the data internally. But the recipient of the information will not be able to identify the individuals either from the data themselves, or from the data plus any other information held by the Agency, because the recipient will not have access to that other information. For the purpose of this particular act of processing, therefore, which is disclosure of these data in this form to these people, no living individual to whom they relate is identifiable. I am afraid that this may not be exactly the same route as that taken by either of my noble and learned friends, Lord Hope of Craighead or Lord Rodger of Earlsferry, but for practical purposes this may not matter and I have no wish to add further confusion to this already confusing case by elaborating.

93. If, of course, barnardisation is not effective to protect individuals from the risk of identification, then the information can only be

disclosed in accordance with the data protection principles. On this subject I have nothing to add to the observations of Lord Hope and Lord Rodger.

94. I too, therefore, would allow this appeal and make the order proposed by Lord Hope.

LORD MANCE

My Lords,

95. I have had the benefit of reading in draft the opinions of my noble and learned friends, Lord Hope of Craighead and Lord Rodger of Earlsferry, and I agree with them that the appeal should be allowed and the order proposed by Lord Hope made.

96. The only significant difference in the reasoning of my noble and learned friends relates, as I see it, to the interpretation and so application of part (b) of the definition of "personal data" in s.1(1) of the Data Protection Act 1998. Both take the view, as I do, that part (a) relates to the particular data under consideration, that is, in this case, the barnardised data. Lord Rodger takes the view that part (b) is irrelevant, because the "other information" to which it refers only embraces "other information" which is not itself "data" in the possession of the data controller at the time of processing. Lord Hope takes the view that "other information" in part (b) covers all other information including data other than the particular data under consideration for processing (here the barnardised data). But he concludes that this makes no difference because part (b) only contemplates a situation where the particular data under consideration and the "other information" each have a contribution to make to the result (that is the potential identification of a living individual).

97. It is unnecessary in this case to decide between these rival views, but my own preference is for Lord Hope's. In all other respects, I also agree with his reasoning.