

THE INTERFACE OF FREEDOM OF INFORMATION AND DATA PROTECTION

Timothy Pitt-Payne

(Barrister, 11KBW; Visiting Professor of Information Law, Northumbria University)

In this paper the Freedom of Information Act 2000 is referred to as "FOIA"; the Environmental Information Regulations 2004 as "EIR"; and the Data Protection Act 1998 as "DPA".

HOW MANY HATS CAN RICHARD THOMAS WEAR?

1. If you visit the UK Information Commissioner's website¹ you will see the following statement at the head of the home page:

The Information Commissioner's Office is the UK's independent authority set up to promote access to official information and to protect personal information.

2. The "mission statement" is not surprising. The Commissioner is the data protection regulator for the whole of the UK; he is *also* the regulator for the freedom of information regime that applies to England, Wales and Northern Ireland (though not for the separate statutory regime that applies in Scotland²). To add to the mix, he is also responsible for enforcing the UK regulations implementing our EU obligations in respect of environmental information.
3. Yet there is an apparent tension here. The Commissioner exists to *promote access* to one kind of information, namely official information. The two obvious ways to promote access to information are, first, by encouraging those who hold the information to take active steps to publish it, and, secondly, by encouraging them to make it available on request. The Commissioner, of course, has a statutory responsibility to promote access

¹ <http://www.ico.gov.uk/>

² Under the Freedom of Information (Scotland) Act 2002. See further the discussion below of the *CSA v Scottish Information Commissioner* case in the House of Lords.

to official information in both of these ways³. Yet the Commissioner also exists to *protect* another sort of information, namely personal information. The obvious way in which you protect information is by limiting access to it, or by limiting the use that can be made of it. Again, the Commissioner has a statutory responsibility to protect personal information in both of these ways⁴.

4. One way of avoiding any conflict between these two objectives would be to define “official information” and “personal information” in such a way that the two categories were mutually exclusive. This is not the approach that UK law has taken. What makes information “official information” for the purposes of FOIA and EIR is the fact that it is held by particular kinds of bodies, namely public authorities⁵. What makes information “personal information” is the fact that it relates in particular ways to ascertainable living individuals⁶. Clearly, if a public authority holds personal information, then the same item of information will be both official information and personal information.
5. Rather, the key to resolving any conflict (or apparent conflict) is to recognise that the two legislative objectives reflected in the statement from the Commissioner’s website are not absolute. UK law *does* promote access to official information: it does so by FOIA and EIR (in relation to which the Commissioner has enforcement responsibilities), and by other legislation for which the Commissioner is not responsible⁷. But the right of access is not absolute: there are a number of restrictions, including the various exemptions in FOIA Part II and in EIR regulations 12 and 13.
6. Likewise, UK law protects personal information: most obviously by the DPA, but also by the law in relation to breach of confidence, and by the Human Rights Act 1998⁸. Again,

³ In relation to publication, see FOIA sections 19-20 (publication schemes); in relation to requests for information, see FOIA section 1, and section 50 (complaints to Commissioner if requests for information not dealt with in accordance with requirements of the Act).

⁴ See DPA section 4 and Schedule 1, for data controller’s duty to comply with the data protection principles; see generally Part V of the Act for the Commissioner’s duty in enforcing those principles.

⁵ As defined in section 3 of and Schedule 1 to FOIA. There is a slightly different definition in EIR – see regulation 2(2).

⁶ See the definition of “personal data” in DPA section 1, as discussed in *Durant v Financial Services Authority* [2003] EWCA Civ 1746. In *Durant* the Court of Appeal held that whether data is *personal* data depends on whether it has an individual as its focus, and whether it is biographically significant in relation to that individual: see *Durant* at paragraphs 26-31. But see now the Information Commissioner’s technical guidance on the definition of personal data:

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

The relationship between *Durant* and the guidance remains controversial.

⁷ See for instance the legislation that specifically relates to access to information held by local authorities: e.g. in the Local Government Act 1972.

⁸ From the point of view of personal information, the most important issue about the Human Rights Act is the extent to which it gives further effect to article 8 of the European Convention on Human Rights.

though, the protection is not absolute: there are numerous circumstances in which personal information may be used or shared without the consent of the individual to whom the information relates.

7. Once it is understood that access to official information and the protection of personal information do not operate in absolute terms, then it is easier to understand how UK law can set out promote both objectives, and indeed can do so via a common regulatory framework⁹. The question with which this paper is concerned is how in practice these two objectives have been balanced, in particular since FOIA 2000 came fully into force on 1st January 2005¹⁰.
8. The remainder of this paper falls into three parts. The first part outlines the legal framework. The second deals with some of the practical difficulties to which it gives rise, and suggests a solution. The third looks at some of the relevant cases that have been decided in 2008.

PART 1: FOIA 2000 AND ACCESS TO PERSONAL INFORMATION - THE LEGAL FRAMEWORK

9. The main relevant provision in FOIA 2000 is section 40: this creates a number of related exemptions from the general right of access under section 1 of the Act. The provision is a complex one; the most important point is the difference between two kinds of requests to public authorities involving access to personal data, dealt with by section 40(1) and section 40(2) – (4) respectively.

First kind of request: personal information about the requester

10. The first kind is a request for personal data *about the requester himself*. Information will be absolutely exempt from disclosure under FOIA 2000 if it constitutes personal data of which the applicant is the data subject¹¹. At first sight this is very surprising indeed: individuals have a strong and obvious interest in access to personal information about themselves.

⁹ Not only does the Information Commissioner have a role in giving effect to both objectives, but so does the Information Tribunal.

¹⁰ EIR came into force at the same time.

¹¹ See FOIA 2000 section 40(1), read in conjunction with section 2(3)(f)(i). The terms “personal data” and “data subject” are defined in DPA 1998.

11. In fact however, this is a technical provision, a form of legal “traffic flow management”. Its purpose is to ensure that requests by individuals for access to personal data about themselves are dealt with as subject access requests under DPA 1998¹² rather than as information requests under FOIA 2000. The exemption is not intended to exclude individuals altogether from having a right of access to any personal information about themselves that is held by public authorities.
12. In some important respects an individual seeking access to his own personal data is in a stronger position where the data controller is a public authority¹³ than in relation to data controllers generally. For the purposes of the right of subject access, the definition of “data” is wider in respect of public authorities than in respect of data controllers generally, and extends to all recorded information held by the public authority¹⁴. The extended definition of data in respect of public authorities is contained in DPA 1998 section 1(1)(e). Hence the range of information that can be obtained by a subject access request is potentially greater when the data controller is a public authority.

Second kind of request: personal information about third parties

13. The second kind of involves requests for access to *third party* personal data (that is to say, information that is personal data about someone other than the individual who is making the request). It is in relation to this second kind of request that the potential conflict between privacy objectives, and the right of access to governmental information, becomes acute.
14. Section 40 creates the following exemptions applicable to requests for access to third party personal data¹⁵.
- An **absolute** exemption, where disclosure of the information to a member of the public otherwise than under FOIA 2000 would contravene any of the data protection principles: see FOIA 2000 section 40(3)(a)(i) and 40(3)(b).

¹² See DPA 1998 section 7 for the right to make requests for access to personal information about oneself.

¹³ The term “public authority” in DPA 1998 has the same meaning as in FOIA 2000: see DPA 1998 section 1(1) as amended by FOIA 2000 section 68(2)(b).

¹⁴ Some information falling within section 1(1)(e) is categorised as “unstructured personal data” under section 9A(1) of DPA 1998: in which case, the right of subject access is limited in the respects set out in section 9A(2)-(6).

¹⁵ FOIA 2000 section 2(3)(f) determines which of these exemptions are absolute and which are qualified.

- A **qualified** exemption, where disclosure of the information to a member of the public otherwise than under FOIA 2000 would contravene section 10 of DPA 1998 (the right to prevent processing likely to cause damage or distress): see FOIA 2000 section 40(3)(a)(ii).
- A **qualified** exemption, where the information is exempt from the data subject's own right of subject access by virtue of any of the provisions of DPA 1998 Part IV: see FOIA 2000 section 40(4).

15. The exemption that has given rise to most discussion so far both in the Information Commissioner's decisions and in appeals to the Information Tribunal is the absolute exemption relating to information the disclosure of which would contravene any of the data protection principles. At first sight the absolute nature of this exemption might suggest that the values inherent in the data protection principles will "trump" those inherent in FOIA 2000: in other words, where there is a conflict then protecting personal information takes precedence over promoting access to official information. This would be a superficial and misleading approach to section 40. The data protection principles are themselves open-textured, and intended to accommodate conflicting interests. As the cases discussed below illustrate, what both the Commissioner and the Tribunal have done is to consider the competing interests of individual privacy *versus* transparency and open government, accommodating that consideration within the framework of the data protection principles themselves. The result is that there have been a number of occasions on which public authorities have been required to disclose personal data, in particular in relation to their own employees or office holders.

16. In theory all eight data protection principles in Schedule 1 to DPA 1998 are potentially relevant to the operation of the exemption in section 40(3) of FOIA 2000. In practice, so far both the Commissioner's decisions and the Tribunal case-law have mainly focused on the first principle.

17. That principle requires that personal data must be processed¹⁶ fairly and lawfully; that personal data must not be processed unless one of the conditions in Schedule 2 to DPA 1998 is met; and that sensitive personal data¹⁷ must not be processed unless one of the conditions in Schedule 3 is also met.

¹⁶ "Processing" personal data would include disclosing it: see the definition of "processing" in section 1(1) of DPA 1998.

¹⁷ Defined in DPA 1998 section 2.

18. In order to meet the fairness requirement in the first data protection principle, it is necessary to comply with the specific provisions of Schedule 1 Part II paragraph 2. The data subject must be provided with or have made readily available to him certain information in relation to the processing of his data, specified in paragraph 2(3). A notice containing this information is often referred to as a “fair processing notice” (although this term does not appear in DPA 1998 itself). However, the provisions in paragraph 2 are not intended to be an exhaustive definition of what amounts to “fairness” for this purpose. Even where there is compliance with paragraph 2 then the processing may still be unfair on general grounds¹⁸.

19. As far as the Schedule 2 conditions are concerned, the Commissioner’s decision notices and the Tribunal’s case law have often referred to condition 6. This condition is satisfied if:

The processing is necessary for the purposes of legitimate interests pursued 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.

PART II: SOME PRACTICAL PROBLEMS

20. The difference between requests for one’s own personal information (dealt with as subject access requests under DPA) and requests for third party personal information (dealt with under FOIA, but subject to the exemptions in section 40(2) – (4)) gives rise to real practical consequences. There are procedural complications; there are also important differences in the rights available to individuals to challenge decisions by public authorities as to what information should be disclosed.

21. Take a case where an individual makes a disclosure request to a public authority. Some of the information is his own personal data; some of it is third party personal data; and some is not personal data at all. The requester is unlikely to be concerned about these distinctions, and indeed may not be aware of them at all. From his point of view it is likely that all he is interested in is obtaining the requested information, as quickly and simply as possible.

¹⁸ See e.g. *Johnson v Medical Defence Union* [2006] EWHC 321(Ch), at paragraph 114 onwards.

22. Assume that the individual is not satisfied with the authority's response, and complains to the Commissioner. What is likely to happen is that the Commissioner will identify what part of the request relates to the requester's own personal data, and what part relates to other sorts of information. The Commissioner will investigate, and at the end of the investigation will issue a decision notice under section 50 of FOIA. The decision will record that to the extent that the request is for the requester's own personal data the information sought is exempt from disclosure under section 40(1) of FOIA; the decision will then go on and deal with the other information, and the extent to which it is exempt from disclosure, and will set out whether the Commissioner is ordering disclosure of any or all of that information.
23. In addition, the Commissioner may carry out a wholly separate process in relation to the part of the request that constitutes the requester's personal data. That part of the request ought to have been treated by the public authority as a subject access request under DPA section 7. So the Commissioner may carry out an assessment under DPA section 42 as to the way in which the public authority has processed the requester's personal data; and in some cases the Commissioner may choose to require disclosure of personal data, by issuing an enforcement notice under DPA section 42. In our hypothetical case therefore there are two different possible legal routes by which the Commissioner may require information to be disclosed.
24. If the requester appeals to the Information Tribunal then the procedural complexity will continue. The Tribunal will need to determine what part of the request did relate to the requester's own personal data. However, in relation to this part of the request the Tribunal will have no jurisdiction to determine what information should be disclosed. The Tribunal has no jurisdiction to entertain a complaint by a requester that his rights under DPA section 7 have been breached; nor has it any jurisdiction to hear an appeal by a requester against the Commissioner's assessment under DPA section 42, or against the Commissioner's decision not to take enforcement action under DPA section 40.
25. In relation to the other information covered by the request, the Tribunal has extensive powers on appeal (allowing it to substitute its own view for that of the Commissioner on questions of law, fact or discretion) and it can therefore require disclosure of information in cases where the Commissioner has declined to do so: see FOIA sections 57 and 58.

26. The structure as set out above is cumbersome and complex: the Commissioner deals with different elements of the same request by means of two different processes, and the Tribunal lacks jurisdiction to deal with all of the issues arising out of the request.
27. In addition there is a surprising disparity as between the rights available to the person seeking their own personal data and the person seeking other sorts of information from a public authority. The requester seeking his own personal data, as we have seen, cannot complain to the Tribunal that his rights under DPA section 7 have been breached. His only option is to go to the ordinary courts, facing both the procedural complexity and the costs risks that this entails. On the other hand the person seeking other information from a public authority, if he is not satisfied with the Commissioner's decision on his complaint, can bring an appeal to the Tribunal; this is procedurally (relatively) straightforward and is unlikely to give rise to a costs order against him.
28. A very modest amendment to FOIA could address some of these difficulties. All that would be necessary would be to provide that a complaint could be brought to the Commissioner under section 50 of FOIA, not solely (as at present) in relation to a failure by a public authority to comply with its duties under FOIA, but also in relation to a failure to give effect to the subject access right under DPA section 7. The existing right of appeal to the Tribunal under section 57 could then be left in place, in relation to all complaints brought under the (modified) FOIA section 50. This would enable both the Commissioner and the Tribunal to deal, in a single process, with all issues arising out of information requests to public authorities.
29. What might be objected to the above suggestion is that it creates an unacceptable distinction between the treatment of subject access requests made to public authorities and to other data controllers. In which case, an alternative would be to make similar provision in respect of *all* subject access requests, whatever the status of the data controller – with a right of complaint to the Commissioner followed by a right to appeal to the Tribunal. This has its attractions, but it would also involve a very substantial expansion in the workload of both the Commissioner and the Tribunal.

PART III: RECENT CASES

30. There have now been a number of Tribunal decisions under section 40 of FOIA, and a number of decisions by the Commissioner. I want to look at two in particular from 2008 – one from the High Court and one from the House of Lords.

MPs' expenses in the High Court

31. The High Court case is *Corporate Officer of the House of Commons v Information Commissioner and others* [2008] EWHC 1084 (Admin). This is one of a number of cases arising out of FOIA request for information about MPs' expenses, but it is the only one so far to reach the High Court. The case involved requests for third party personal data (the third parties in question being the MPs themselves).
32. The context for this case was the system of paying Additional Cost Allowance (ACA) to MPs. With the exception of those who represent Inner London constituencies, MPs are entitled to ACA to reimburse the cost of overnight stays away from their main residence. In very many cases ACA is used to defray the cost of a second home – since many MPs have both a London and a constituency home.
33. The House of Commons operates a publication scheme under FOIA, and at the time the requests were made the total amount paid each year to each individual MP by way of ACA was published under this scheme. However, the information was not broken down as between different heads of expenditure.
34. The requests at issue in this case related to the ACA paid to 14 named MPs in particular years. Effectively the requests were for full information about all ACA claims made by these MPs in the relevant years, together with any supporting documentation.
35. The House of Commons refused the requests, on the basis that disclosure of information going beyond what was in the publication scheme would breach the data protection principles, and hence the requested information was exempt from disclosure under FOIA. The requesters complained to the Commissioner, who upheld their complaints in part, requiring disclosure of a breakdown of these ACA payments, year by year, by reference to a number of specific categories. The House of Commons then appealed to the Tribunal contending that no information beyond what was in the publication scheme should have been ordered to be disclosed; and the requesters cross-appealed, contending that the Commissioner should have ordered disclosure of all of the requested information.
36. The Tribunal concluded that all of the information requested should be disclosed, with a few limited exceptions. It considered that the ACA system was very unsatisfactory, with acute shortcomings in terms of transparency and considerable opportunities for abuse.

37. The case against disclosure largely rested on the argument that this would breach the first data protection principle. The Tribunal rejected this: in particular, it held (i) that disclosure would not be unfair to individual MPs, and (ii) that the condition in Schedule 2 paragraph 6 would be satisfied. An important part of the Tribunal's reasoning was that, given the shortcomings of the ACA system, there was a strong public interest in disclosure. This was particularly relevant to the finding in relation to Schedule 2 paragraph 6. In substance the Tribunal's approach was similar to the public interest test applied in respect of the qualified exemptions. The difference though is that the public interest test requires a consideration of competing heads of public interest (the interest in disclosure as against the interest in maintaining the relevant exemption); to the extent that there is a balancing exercise in section 40 cases, what is being weighed against any public interest in disclosure is the *individual privacy interests* of the data subjects concerned (i.e., in this case, the MPs).

38. The appeal to the High Court by the House of Commons was rejected. The High Court emphasised the limited nature of its jurisdiction. Unlike an appeal from the Commissioner to the Tribunal, an appeal to the High Court could be brought solely on the basis of error of law:

This court has no jurisdiction to interfere with the decision of this specialist Tribunal unless it is legally flawed (see paragraph 6 of the decision: emphasis in original).

39. The main ground of appeal was that the Tribunal misdirected itself by failing to give appropriate weight to the reasonable expectations of MPs about precisely how information about the ACA claims would be made available to the public. This was rejected by the High Court, primarily because this was a consideration that the Tribunal had expressly considered and rejected, by reference to the facts, and there was no error of law entitling the High Court to interfere. The High Court also rejected an argument that the Tribunal ought to have withheld MPs' private residential addresses from disclosure: again, there was no error of law in this conclusion.

40. The High Court's discussion of the data protection principles is confined to the first principle, and is mainly focused on whether condition 6 in Schedule 2 was satisfied. The Court recorded (see paragraph 43 of the decision) that it was common ground that condition 6 required a consideration of whether there was a pressing social need for

disclosure, and whether the interference was proportionate as to means and fairly balanced as to ends. It referred to the approach taken by the European Court of Human Rights to interference with a recognised right, and cited *Sunday Times v UK* (1979) 2 EHRR 245 at paragraph 59. The adjective “necessary “ was not synonymous with “indispensable”, but nor did it mean simply “reasonable” or “desirable”. In the present case the High Court considered that the Tribunal was entitled to find that this test was satisfied, given the public interest considerations that it had identified in favour of disclosure of the requested information. Essentially, the Tribunal was entitled to find that disclosure to the public met a pressing social need, and that the individual privacy interests of MPs were not sufficient to outweigh this and preclude disclosure.

41. There is however something of a hint (see paragraph 44 of the decision in particular) that if the arrangements for oversight and control of the ACA system were to change then that might lead to a different conclusion in the future.
42. Subsequently FOIA was modified by the *Freedom of Information (Parliament and National Assembly for Wales) Order 2008* (SI 2008 No 1967) so as to exclude certain information in relation to members of either House of Parliament (including information about any residential address) from the scope of FOIA. The Order came into effect on 23rd July 2008.

Health information in the House of Lords

43. *Common Services Agency v Scottish Information Commissioner* [2008] UKHL 47 received some attention, as the first House of Lords case to consider both freedom of information and data protection. This was an appeal from a decision of the Scottish Commissioner under the Freedom of Information (Scotland) Act 2002 (“FOISA”). Although FOISA is not identical to FOIA, the provisions and overall structure are very similar. Both the Ministry of Justice and the UK Commissioner intervened before the House of Lords.
44. The case concerned a request for information about incidents of childhood leukaemia year by year for the Dumfries and Galloway postal area, broken down by census ward. The context was that there was concern about the health risks arising from operations at an MOD firing range in the area, together with nuclear processing at Sellafield and at Chapelcross. The public authority (“the CSA”), an NHS body, refused disclosure on the basis that the low numbers involved meant that there was a significant risk of the indirect

- identification of individuals if the information were to be disclosed. The Scottish Commissioner considered that disclosure of the requested information would breach the first data protection principle (primarily on grounds of fairness to the individual data subjects, i.e. leukaemia patients).
45. However, he also considered the possible application of a statistical technique known as barnardisation. The information requested can be regarded as a series of cells (each cell being the figure for a particular census ward in a particular year). Barnardisation is a technique for random modification of the numerical value of these cells, in order to reduce the risk of disclosure of information about individuals. If the figures were disclosed in barnardised form, then the true numerical value of each cell would not be made public. However, what would be made public would be: (i) whether the numerical value of each cell was zero or not; and (ii) for non-zero numerical values, the *range* within which the true value fell.
 46. The Scottish Commissioner ordered the CSA to disclose the requested information, in barnardised form. The CSA appealed unsuccessfully to the Court of Session, and thence to the House of Lords.
 47. The main questions for the House of Lords were: (i) whether barnardised information was information “held” by the CSA for the purposes of FOISA; and (ii) whether barnardised information would constitute personal data.
 48. On the first question, the CSA contended that the disclosure ordered by the Scottish Commissioner would require it to produce or make new information not held by it at the time of the request, and that this went beyond its obligations under FOISA. The House of Lords rejected this. Provision of barnardised information was comparable to redacting a document; it did not involve the creation of new information, but rather the presentation of existing information in an edited form.
 49. On the second question, the House of Lords considered that the Scottish Commissioner had not properly considered whether the barnardised information constituted personal data or not, and remitted the case for reconsideration. The essential question was whether barnardisation rendered the information fully anonymous, so that the data subject was no longer identifiable from that information. If yes, then the barnardised information would not constitute personal data, and so its disclosure would not need to be

tested against the data protection principles. If no, the information would remain personal data and the application of the data protection principles would need to be considered.

50. In order to reach this conclusion, the House of Lords needed to deal with an argument based on the definition on “personal data” in DPA section 1(1). The definition is 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
[emphasis added]

51. In this case the data controller (the CSA) held information as to the identities of the individual children to whom the barnardised information would relate. Hence, it was argued, in the hands of the CSA the barnardised information would still be personal data; and the disclosure of that information would still constitute the processing of personal data.

52. Their Lordships rejected this argument. See e.g. the speech of Lord Hope, at paragraph 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.

53. This was a conclusion that all the members of the House of Lords clearly wanted to reach on pragmatic grounds. They did not wish to see a position whereby all releases of anonymised health statistics (whether made voluntarily or in response to a FOIA/FOISA request) would need to be tested against the data protection principles. In particular, they were concerned that if such information counted as personal data then it would also be sensitive personal data, and so a Schedule 3 condition (as well as a Schedule 2 condition) would need to be satisfied.
54. However, it is clear that all of their Lordships recognised that the language of DPA section 1(1) was a serious obstacle to reaching this result. Their solutions to the problem differ, but the strongest support was for the approach adopted by Lord Hope: Lord Hoffman agreed with his speech, and Lord Mance (while not deciding the point) expressed a preference for Lord Hope's approach as against the somewhat different reasoning of Lord Rodger.
55. The key passage in Lord Hope's speech, as far as the construction of DPA section 1(1) is concerned, is paragraph 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 anonymised, 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.

56. None of their Lordships was assisted by the *Durant* case (which the Court of Session had relied upon heavily in its decision). However, nor did the House of Lords adopt the

invitation by the UK Information Commissioner and the Ministry of Justice, in their respective interventions, to give specific endorsement to the UK Commissioner's technical guidance on the meaning of personal data. The relationship between that guidance and the *Durant* case therefore still awaits authoritative resolution. Issues as to what constitutes personal data are central to the operation of the DPA generally; but they are also of very great importance for FOIA, as the discussion in this paper will I hope have made clear.

December 2008