Subject Access and government secrecy

some thoughts based on *Lord Ashcroft v Attorney-General*

for Masons Update Seminar, 13 January 2004

Mark Warby QC

1. This paper has its origins in a talk I gave to the Sweet & Maxwell Privyacy LawSeminar, 'Access to Information', held at Masons in November 2003, based largely on my experience as Counsel for Lord Ashcroft in his data protection claims against government departments. The paper has been amended and updated to take account of the specialist nature of this audience, and to include consideration of the subsequent decision of the Court of Appeal in *Durant v Financial Services Authority* [2003] EWCA Civ 1746 and its impact on this area of law.

Lord Ashcroft v Attorney-General & DfID: outline facts

2. Lord Ashcroft, as he now is, was the Treasurer of the Conservative party 1998-2001. He was also a major donor to the party. During 1999 and 2000 he was the target of a great deal of hostile publicity in the press, much of it based on leaks from UK government officials and files. As part of a series of defamatory publications in The Times during the summer of 1999 articles appeared based on documents from files at the Foreign Office (FCO) which contained disparaging remarks about him by civil servants. Later, documents from the files of the Department for International Development (DfID), recording an embarrassing dispute between him and the High Commissioner in Belize were leaked to the Guardian. And information about the fate of his nominations for a working peerage was leaked to the press also; it was reported that his first nomination had been rejected and that his second nomination had been recommended against by the Political Honours Scrutiny Committee. Michael Ashcroft was appointed a working peer in April 2000.

3. Lord Ashcroft sued The Times for libel over articles based on leaked (and inaccurate) information from US sources, and secured an apology. For the rest, he was convinced that he had been the target of a politically motivated and malicious campaign by members of the Labour government, aimed at damaging the Tory party and its electoral prospects by discrediting him, and thereby undermining Tory party finances. He wanted to find out who had leaked against him, and who had induced the PHSC to advise against his appointment. His starting point was to make SARs to the FCO, DfiD and the Cabinet Office. Later, he brought three actions.

(1) A claim for damages in respect of the leaks from FCO[1] and DfiD, based principally on rights of confidence/privacy, but including claims for compensation under the DPA. Also included in this action was a claim for damages for misfeasance in public office against one individual FCO official who appeared to have (at the least) confirmed the authenticity of a leaked document to the press.

(2) A second claim against the FCO (see n1) and DfID, which the court directed him to pursue separately, for further and better access to data held by them. This claim relied on s7 DPA, Article 8 ECHR and the HRA. Lord Ashcroft's contention was that the defendants' SAR responses were inadequate, and non-compliant with his rights under the DPA..

(3) A claim against the Cabinet Office for relief of the same nature, and on the same basis as the second claim against FCO/DfID. This action was concerned with information about his peerage nominations, which he had been denied.

4. It was the second of these three actions that came to trial before Gray J in May 2003. That was after *Durant* had been decided at first instance, but before the hearing in the Court of Appeal. It was also before the decision of Munby J in *R(Lord) v SSHD.* The trial opened, but on day 2 of an estimated 5 day trial that case and both the other Ashcroft actions mentioned were settled by means of an apology from the defendants and a substantial payment by them in respect of Lord Ashcroft's costs.

5. The *Ashcroft* case is therefore authority for nothing. And some of the arguments advanced have now been the subject of decision by the Court of Appeal in *Durant,* where the FSA ran the same legal arguments as the *Ashcroft* defendants (using the same Counsel) had put forward. But

(1) not all of the points raised in *Ashcroft* were dealt with in the *Durant* judgments;

(2) on some of the issues *Durant* did tackle there remain some points of interest and potential importance;

(3) *Ashcroft* provides in any case a startling illustration of some of the consequences of the *Durant* rulings.

Ashcroft: the issues

6. Five main issues arose:-

(1) the meaning of 'relevant filing system'

(2) the meaning of 'personal data'

---

[1] The defendant to this claim was the Attorney-General, the correct defendant under the Crown Proceedings Act.

(3) the third party data provisions in s7(4)-(6) DPA; proper interpretation and application
(4) the validity and applicability of some of the DPA exemptions
(5) access rights under the Directive and ECHR/HRA.

The European legal context

7. The first three issues I have mentioned obviously involve construing the provisions of DPA ss.1 and 7, but the arguments developed in *Ashcroft* recognised, as they had to, that the DPA cannot and should not be construed in isolation.
   (1) First, and most obviously, the Act must be construed in the light of, and in conformity with, the Directive that it was intended to implement, Directive 95/46/EC. This was acknowledged in *Durant*, though it can certainly be argued that the court did not pay close enough attention to some aspects of the Directive.
   (2) Secondly, the ECHR and the Human Rights Act may have an impact on construction. Recital 10 to the Directive acknowledges the aim of protecting the right to privacy under Article 8 of the Convention. And Strasbourg authority shows that it can be an interference with an individual's rights under Article 8 for a state to store and/or use personal information about an individual, and then refuse him access to it: see *Leander v Sweden* (1987) 9 EHRR 433, [48]; *Amann v Switzerland* (2000) 36 EHRR 843, [69] & [80]; *Rotaru v Romania* (2000) 8 BHRC 449, [43]-[44], [46]. By s3 of the HRA the access rights under the DPA must be construed, if possible, compatibly with Article 8. Even an unreasonable construction can be adopted, where necessary to ensure compatibility: *R v A* [2002] 1 AC 45. This aspect of the matter did not attract any attention in the *Durant* judgments.

8. It was this same European legal context that threw up the other issues mentioned at 6 above.
   (1) EC Directives can of course have direct effect, provided certain conditions are met. And it had already been held, before the *Ashcroft* hearing, that Article 14 of the Data Protection Directive does have direct effect: *R (Robertson) v Wakefield MDC* [2002] QB 1052. So, it was argued, if the access rights granted by the DPA fall short of those guaranteed by the Directive Lord Ashcroft was entitled to invoke the rights guaranteed by the Directive itself. Similarly, if the DPA contained exemptions from access which were not authorised by the Directive Lord Ashcroft was entitled to object to the state's reliance on those exemptions. Neither of these issues was covered by the judgments in *Durant*.
   (2) Similar points were advanced in reliance on Article 8 ECHR and ss6 & 7 HRA: if Article 8 gives rise to a right of access the English court is obliged by s6 to grant the appropriate remedy. If the DPA does not extend far

enough to allow that to be done the court can grant the remedy under s7 HRA. Similarly, a provision of the DPA which exempts data from access which *would* otherwise be available may be vulnerable to an argument that it is incompatible with Article 8. Again, these points were not touched on in the *Durant* judgments.

(1) 'Relevant filing system'

9. As is well known, apart from information in 'accessible records' as defined in DPA s1(1)(d) the only manually recorded data to which s7 DPA *presently* affords access are personal data recorded as part of a system which falls within the meaning of this term. The position is due to change in a year's time when amendments to the DPA introduced by ss68 & 69 of the Freedom of Information Act take effect, and unstructured data held by public authorities becomes accessible under s7 (see below). But for the time being this is the crucial term, the interpretation of which governs the extent of access available to manual files which are not 'accessible records'. It is the subject of a lengthy and complex definition in DPA s1(1), with which readers of this paper will be familiar.

> 'Relevant filing system' means [a] any *set of information* [b] *relating to individuals* to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is [c] *structured,* either *by reference to individuals, or* by reference *to criteria relating to individuals,* in such a way that [d] *specific information* relating to a *particular individual* is *readily* accessible.

(The emphasis has been added and lettering interpolated)

10. The argument advanced by the defendants in *Ashcroft* and again by the defendants in *Durant* was that the definition is of limited scope: each of the criteria lettered [a] to [d] above must be met; so the definition only catches highly structured files or systems, being those which are organised and structured in such a sophisticated way that a specific kind of information about a particular individual is accessible with the same or a similar degree of ease as would be the case with a computerised system. In practice, this means only systems which involved categorisation of information by reference both to individuals, and by reference to subject-matter. Three principal lines of argument were these:

(1) the wording of the definition (and in particular the formula "although the information is not processed by means of equipment .." etc) shows a clear intention to ensure that it only covers filing systems which are comparable to computer systems as regards ease of access to specific information about a given individual;

(2) the promoters of the bill made clear in parliamentary statements that the definition was meant to be of limited scope and was not even meant to catch 'files about named individuals' if they were files 'where a variety of

different kinds of documents is stored by date order' (The late Lord Williams, HL Debs, vol 585, 2 February 1998, col 438; HL Debs, vol 587, 16 March 1998 col.467);

(3) a narrow interpretation can be explained and justified by reference to the practical reality of the searches which have to be made to comply with SARs and the relatively short 40 day timescale for response; the officer concerned, who may know little or nothing about the individual making the SAR, needs to be able to find information with a minimum of effort.

11. The Court of Appeal in *Durant* was seduced by these arguments, and its conclusions (see [45]-[50], esp para [50]) essentially adopted all of the arguments of Counsel for the FSA. The consequence seems to be that, for the moment at least, if the state keeps badly organised filing systems, or even well-organised systems structured by reference to topics rather than individuals, then there is no right of subject access under the DPA. Worse, there will be no access right even if papers are filed under individuals' names and particular information within them is readily accessible in practice, *unless* the documents are *also* broken down by tabs or flags into kinds of information, such as health, conduct in employment, etc.

12. The impact of this in practice can be illustrated by reference to the facts of *Ashcroft.* The FCO, which admitted that documents from its files had been leaked to the press, held no less than 41 files containing 'hundreds of references' to Lord Ashcroft. Of these, several were files with his name on the outside. Others were labelled as relating to topics to which he was clearly central. Civil servants had been able to obtain documents from these files and leak them. There was also evidence that officials had, without apparent difficulty, prepared memoranda about Lord Ashcroft based on scrutiny of these files. But the FCO generally organises its filing systems by reference to subject matter, not individuals. Nor did the named or topic files which did exist have tabs or other means of readily identifying papers which related to Lord Ashcroft, or specific types of information within them. So Lord Ashcroft was denied access to all the information in all these files. The *Durant* ruling endorses the FCO's approach in *Ashcroft.*

13. This is troubling, because that approach enabled the government initially to conceal from Lord Ashcroft some important information about the leaks against him. We only know this for sure because, in the first of the actions I have mentioned - the damages claim - Lord Ashcroft obtained disclosure under the CPR. This disclosure included copies of some manual records which the FCO and DfID had withheld in response to Lord Ashcroft's SARs. The manual records disclosed included a considerable volume of documentation evidencing and relating to the detailed inquiry which the government had carried out into the leak of FCO documents to The Times. Amongst those documents were some containing the evidence on which Lord Ashcroft based his claim against the individual civil

servant, for misfeasance in public office - an important issue, and one of real public interest.

14. A number of arguments can be advanced in support of the view that the interpretation of'relevant filing system' accepted in *Durant* is too narrow. But most of them were advanced on behalf of Mr Durant, unsuccessfully. So it seems improbable that the proper interpretation of 'relevant filing system' can now be revisited in any domestic court short of the House of Lords. I see only three possible ways in which, in the CA or below, the *Durant* ruling on this point could be evaded or overcome.
    (1) First, it does not appear from the judgment that the Court considered the impact of Article 8 ECHR on the question of interpretation. It could perhaps still be argued that the decision was to that extent *per incuriam*, and an attempt made to persuade the court that s3 HRA requires a generous interpretation to be placed on 'relevant filing system' so as to ensure that the DPA gives full effect to the rights of access to government information which Article 8 undoubtedly implies in some cases.
    (2) Alternatively, and perhaps more realistically, reliance could be placed in an appropriate case on the Article 8 access right itself, as a free-standing right of access to information, however recorded, falling outside the DPA.
    (3) Finally, it is possible that the ECJ may at some point pronounce on the meaning of the corresponding provisions of the Directive in a way which conflicts with the CA's ruling. In that case - since the DPA is meant to implement the Directive - English courts at all levels would surely be bound to apply the ECJ ruling in preference to *Durant*, whether that be by re-interpreting the DPA or by giving direct effect to the Directive (a subject I return to later on).

15. It seems unlikely, however, that any case will arise in the next 12 months in which any of these arguments can be tested in court. Once the DPA is amended in January 2005 they will probably cease to be relevant, in the context of government information. The third point will remain of some relevance, in relation to access claims against a private law person or body.

(2) 'Personal data'

16. It is of course 'personal data' that is the primary information accessible under s7. It is the meaning and application of this term that determines whether, if a given type of record qualifies as 'data', information from that record is accessible to an individual and, if it is, how much. Personal data is defined in s1(1) as data 'which *relate to* an individual who can be identified ...' The statutory definition has no inbuilt limitations, such as relevance or subject-matter. As Jay & Hamilton have observed, the definition appears to be a very broad one.

17. It was part of Lord Ashcroft's argument that the definition should be given the broadest possible construction, whereas the government departments he sued had taken a very restrictive view of what was personal data. Much of the computerised information which they did disclose to him had been drastically redacted prior to disclosure, so that - to take an extreme example - from one 3-page document everything but Lord Ashcroft's name was redacted. Another document, a letter from Michael Ancram to the FCO asking about the leak inquiry relating to Lord Ashcroft, was drastically cut. It appeared that the main criterion adopted was that disclosure would be given of information which referred to Lord Ashcroft by name, but not otherwise. And where disclosure was given, it would generally be restricted to the sentence or phrase in which his name appeared. A related complaint of Lord Ashcroft was that redaction as extreme as this violated the requirement of s7 that disclosure should be in an intelligible form. This approach was challenged on a number of bases, among them being the obvious point, that if 'relate to' had been intended to mean 'refer to' then Parliament would have used the latter words.

18. The FCO and DfiD argued in *Ashcroft* for a narrow construction of 'personal data', and so did the FSA in *Durant*. In the event, the Court of Appeal has approved an interpretation which appears to be narrower even than the one which the defendants were contending for. According to *Durant*

(1) It is *not enough* that information refers to an individual by name; that does of itself not make it his personal data; 'mere mention ... does not necessarily amount to his personal data.'

(2) Whether information is an individual's personal data depends on where it stands on 'a continuum of relevance or proximity to the data subject';

(3) One notion 'that may be of assistance' is 'whether the information is biographical in a significant sense';

(4) A second is that of 'focus'; 'The information should have the data subject as its focus'.

(5) 'Personal data' is information 'that affects [the data subject's] privacy'.

Although this was not spelled out, another notion to which the Court of Appeal evidently considered data controllers should have regard is the concept of data ownership. A repeated theme of the relevant passages of the *Durant* judgment is that data is only accessible to a person if it is '*his* personal data'.

19. The introduction of the these numerous evaluative tools into the application of a definition that would appear on its face to be broad and value-neutral is liable to be problematic and, I would suggest, defeat some of the desirable aims of the data protection legislation. First, data controllers are given a difficult task to perform in deciding what they must disclose. Apparently they must or can now ask themselves such questions as "Where on the continuum of relevance or proximity does this data lie?" "Is it biographical in a significant sense?". "Is the applicant the focus of the data?" Secondly, the reality is that data controllers will err on the side

of non-disclosure, and it will be difficult to challenge their decisions. By definition, data subjects will rarely have enough information to be confident about the merits of such a challenge. One wonders also what view the court will take of its task where such a challenge is mounted. Is the task to be one of second-guessing the data controller, and deciding the same issue afresh? Or is the court to defer to the data controller in this respect (cf the Court of Appeal's approach to review of a data controller's decision on the redaction of third party information, at [60]-[61])?

20. Some of the dangers of a narrow approach to what is 'personal data' are illustrated by *Ashcroft*, where Lord Ashcroft eventually obtained through disclosure complete versions of documents which had been provided earlier in heavily redacted form. It was therefore possible to determine exactly what had been redacted. Some of the redactions resulted in the concealment of information of great importance to the claims Lord Ashcroft eventually pursued. Some of these redactions were later reconsidered by the defendant departments, which conceded that their earlier cuts had gone too far. It is a matter for speculation whether all these concessions would have been made if Lord Ashcroft had not started his claim for damages and obtained full copies of the documents via disclosure in that case.

21. I readily confess that I am startled by the Court of Appeal's approach, which seems to me wrong for a number of reasons. I am baffled, for instance, as to how the court reconciles its view that information is not necessarily personal data even if it *refers* to a person with Article 2(a) of the Directive which defines personal data as "*any* information relating to an identified or identifiable individual ..." I am puzzled by the suggestion at [28] that the ECJ decision in *Lindqvist* supports the Court's conclusions. The opposite seems to me closer to the truth. But again, it must be acknowledged that the doctrine of precedent restricts the prospects for a litigant in any court short of the House of Lords seeking to challenge the *Durant* decision on the point. What means are available in or below the CA to challenge or get round this ruling? At the moment, these seem the best candidates.

    (1) It may be argued that the decision was *per incuriam* inasmuch as it relied on the argument that the express inclusion of 'expressions of opinion and intention' within the meaning of 'personal data' supported a narrow construction. The argument that appealed to the court was that this provision would have been redundant if a broad construction was intended; such expressions would then fall within the term anyway. But this ignores the legislative history of this wording; parliamentary statements demonstrate that the reference was included for the avoidance of doubt(!). As Jay & Hamilton observe, in a passage not mentioned in the judgments, the words relied on by the court 'are mere surplusage'. This argument would need to be allied with others, as this was but one of several grounds relied on by the court. But it would at least afford a court a respectable basis on which to depart from *Durant*.

(2) A point that does not seem to have been addressed to, or by the court in *Durant* is the well-established principle that if the same term appears in several places in a statute it should be given the same meaning. Thus, if information only 'relates' to A for the purposes of s1(1) and 7(1) when it has A as its 'focus' and is significant biographical information, a similar approach must be taken when asking whether personal data contains information 'relating to' another individual for the purposes of s7(4). But *can* information which has A as its focus and is therefore what the Court of Appeal calls '*his* personal data' *also* have B as its focus and be significantly biographical about him? Medical information about twins, yes. No doubt there are other examples, but the circumstances would surely be pretty rare. This suggests that the Court's approach to s1(1) may have been wrong. (Alternatively, it raises an interesting point about the third party exception: see below).

(3) Alternatively, a data subject might seek to get round argument about what is personal data by relying on the other disclosure requirements of s7, and in particular the intelligibility requirement, as a basis for gaining access to information that the data controller alleges is not the data subject's personal data. In *Ashcroft* it was acknowledged, in the end, that some information that was not, on the defendant's approach, personal data relating to Lrd Ashcroft, needed to be disclosed to satisfy the intelligibility requirement. Of course, this only works, if at all, if there is *some* personal data in a document to start with; the obligation to disclose in an intelligible form only arises if this is so.

(4) As mentioned above, a further ECJ ruling on the meaning of the corresponding provisions of the Directive might suffice, if clearly at odds with *Durant.*

(3) Third party data and redaction

22. ss7(4)-(6) DPA contain provisions intended to protect the privacy interests of third parties, information about whom may be included in a disclosure made by a data controller pursuant to a SAR. Issues arose in both *Ashcroft* and *Durant* about the proper application of these provisions. In both cases the issue concerned the redaction of third party *names* from the disclosures. The FCO and DfiD redacted nearly all civil servants' names and also the names of foreign officials and ministers. The redaction meant that Lord Ashcroft was denied knowledge of who it was that had spoken or written ill of him, and between which civil servants that information had been passed. *Durant* ruled on the correct interpretation of the relevant provisions. Again, the ruling took a restrictive view of what a data subject may be entitled to obtain.

23. Section 7(4) is worth quoting, with emphasis on the wording discussed below.

> Where a data controller **cannot** comply with [a SAR] without disclosing information **relating to** another **individual** who can be identified from that information he is **not obliged** to comply with the [SAR] **unless** (a) the other individual has consented to the disclosure ... or (b) **it is reasonable in all the circumstances** to comply with the request without the consent of the other individual**…**

24. The following observations can be made about the emphasised words, and the impact of *Durant*.

(1) s7(4) is only engaged where disclosure of third party information would be a necessary consequence of complying with a SAR. In *Durant* Aldous LJ put it differently, suggesting that s7(4) is only engaged where the third party information is necessarily part of the *personal data* that the data controller has to disclose. With respect, that is clearly inaccurate. Disclosure of the personal data itself is only one of the obligations under s7(1). Disclosure of third party information will often be required because of the separate obligation to disclose what the data controller knows about the source of the personal data.

(2) It is only information relating to an 'individual' that is the subject of the exception. A data controller may not withhold information about companies or firms in reliance on s7(4).

(3) The information that can be withheld is information 'relating to' the third party individual. This leads one to examine the implications of the Court of Appeal's narrow approach to the term 'relates to' in s1(1). If information only 'relates to' a person if he is the focus of that information, and it is 'biographical in a significant sense', then the scope of the third party exception must be correspondingly limited. It is only information '*relating to* another individual' that is the subject of the third party exception. So, for instance, if A e-mails B saying that D is a thief, and naming C as his source, the Court of Appeal's approach would appear to recognise that s7 gives D the right to know all of this from A. The information is important biographical information of which D is the focus; so it 'relates to' D. B is the recipient so so s7(1)(b)(iii) applies, and C is the source, so s7(1)(c)(ii) applies. Can A rely on s7(4) to withhold that information about B or C? Surely not. It is A, not B or C who is the focus of the information. Query also whether it is significantly biographical about either of them.

(4) In *Durant* the formula 'not obliged ... unless.... it is reasonable' was held to create a 'presumption or starting point' against disclosure of third party information, albeit one which could be rebutted '*if the data controller considers* that it is reasonable "in all the circumstances" to disclose ...' Two comments arise from this.

i. The use of the word presumption seems to me inappropriate. The statute creates a duty, but then goes on to provide that if condition A is met (compliance with SAR would require disclosure of third party information) the duty does not apply unless condition B (it is reasonable to disclose) is also met. The effect is that the duty *does*

apply if condition B is met, although no doubt the data subject has to prove that this is so.

ii. Even if there is a presumption, condition B in s7(4) is that 'it *is* reasonable' and *not* that the data controller *considers* it is reasonable. The wording implies an objective test.

(5) The court in *Durant* went further, though, and accepted the FSA's submission that it was not for the court to determine whether disclosure is reasonable; instead, it held, the court's function is a reviewing function only, albeit one in which the court will engage in 'anxious scrutiny' of the initial decision.

(6) Apart from the observations mentioned at (4) and (5) above the court in *Durant* was unwilling to lay down any general principles about what would be reasonable in any given circumstances. It gave a few examples whilst observing that, in short, what is 'reasonable in all the circumstances' for the purposes of s7(4) 'all depends on the circumstances': see para [66].

25. The net effect of the court's approach is to give data controllers considerable freedom in making the decision whether to disclose third party information, and to limit severely the room for successful challenge by a data subject to the data controller's decision. It is also difficult to see how this approach can successfully be challenged short of the House of Lords. Having said this,

(1) it may be possible to rely on the argument already outlined, based on the restrictive interpretation of 'relate to' as it appears in s1(1) DPA.

(2) it may also still be possible to advance the argument put forward in *Ashcroft*, that the third party exception is there to protect individual privacy and not government confidentiality; so it is illegitimate to seek to justify withholding third party information in reliance on arguments of the kind deployed in *Ashcroft*, to the effect that disclosure would harm international relations;

(3) alternatively, it can be argued that there is another well-established presumption, namely that governments can only rely on confidentiality where it is shown that disclosure would cause real and substantial harm to the public interest;

(4) information about third parties will still be accessible in any case, if it is of substantial importance to the data subject; for instance, if the information is the identity of a person who has libelled the data subject (unless the journalist's privilege under s10 of the Contempt of Court Act 1981 applies).

(4) Exemptions and their validity

26. The DPA and Statutory Instruments made under it contain a number of exemptions from the subject access right for particular kinds of information. Examples include an exemption for personal data 'to the extent to which [access] would be likely to

prejudice the combat effectiveness of any of the armed forces ...' (DPA Sch 7 para 2) and an absolute exemption for personal data 'processed for the purposes of ... the conferring by the Crown of any honour' (DPA Sch 7 para 3; this was the exemption at issue in Lord Ashcroft's claim). In at least some instances, the validity of such exemptions is open to challenge.

27. Power to grant exemptions derives from Article 13 of the Directive. This authorises the imposition of 'a restriction' on the right of access under Article 12 when it is a 'necessary measure to safeguard' national security, defence, public security and a number of other specified matters. But there are many DPA exemptions for purposes which fall outside the situations specifically mentioned in Article 13. The 'honours' exemption is one of these. Such exemptions are only authorised by the Directive if they fall within the sweeping-up provisions of Article 13(g), which authorises

> ... a restriction [which] constitutes a *necessary measure to safeguard* ... the protection of the data subject or of *the rights and freedoms of others*

28. Any domestic exemption which falls outside the specific areas identified in Article 13(a)-(f) must therefore be tested against the requirements of Article 13(g). If it fails to meet those requirements it will be an unauthorised restriction on the access right under Article 12. Since the UK is bound by EC law to implement that access right, this would lead to the conclusion that the state is not entitled to rely on such an exemption against a subject seeking to enforce the access right.

29. Moreover, the wording of Article 13(g) is clearly similar to and derived from the wording of Article 8(2) of the ECHR. As noted above, Article 8(1) implies some rights of access to information. If the circumstances of a given case are such as to give rise to such rights, the refusal of access will be an interference which has to be justified by reference to the requirements of necessity and proportionality imposed by Article 8(2), or be held incompatible with the Convention.

30. The potential for challenging some of the DPA exemptions on these grounds was recognised by commentators even before the HRA came into force. One exemption identified as potentially falling foul of the HRA was the 'armed forces' exemption mentioned above. That is because it identifies a single criterion for exemption and fails to allow for any balancing of rival considerations. There may be cases where disclosure would probably cause some slight prejudice to combat effectiveness, but other compelling considerations, supported by Article 8, weigh heavily in favour of disclosure. For example, where the information relates to some weaponry which is credibly alleged to cause serious harm to health. cf. *McGinley and Egan v UK* (1998) 27 EHRR 1 (the Christmas Island nuclear test case).

31. Somewhat similar arguments were relied on in *Ashcroft* to challenge the 'honours' exemption. This was said to bar Lord Ashcroft from access to data showing why his initial nomination as a working peer was not accepted. He believed this was due to malicious political interference. An issue arose as to whether the exemption even applied, on its proper construction. But if it did, it was attacked as a blanket and absolute exemption which was very far from satisfying the necessity requirements of Article 13(g) of the Directive or Article 8(2) of the Convention. It is not necessary in a democratic society to impose a complete ban on a person finding out why they have been turned down for legislative office. Such a ban prevents any scrutiny, and permits a secret system to operate in what may be a flawed manner (recent disclosures about the way the New Year's honours list was compiled would tend to support the view that the system is flawed). It is remarkable that a person refused a job as a supermarket shelf-stacker is entitled to see the relevant data in the hands of the prospective employer, subject only to the third party information provisions of DPA s7(4)-(6).

32. In the event, Lord Ashcroft's argument was not tested. But it does seem clear that there is ample scope for challenge to some DPA exemptions, principally deriving from the fact that most of them do not have any built in means of testing the necessity or proportionality of the restriction they impose in a particular case.

(5) Access rights under the ECHR

33. In a case where DPA s7 is held not to apply, because information is on paper records which are neither 'accessible records' nor part of a 'relevant filing system', the *Durant* decision makes it difficult if not impossible to pursue the argument advanced in *Ashcroft*, that reliance could be placed on Article 12 of the Directive itself. But a possible alternative, where the data controller is a public authority, is to rely on Article 8 and the HRA. There is much room for argument about this. So far, as the defendants argued in *Ashcroft*, the Strasbourg Article 8 cases have only found a *positive obligation* of disclosure to exist in a narrowly circumscribed range of cases, where the information at issue affects some *vital interest* of the subject. The cases involve interests close to the core of what Article 8 protects, such as a serious risk to health (see, for instance, *McGinley*, above and *Guerra v Italy* [1998] 26 EHRR 357). But it is surely arguable that the right to reputation is protected to some extent by Article 8; *Rotaru v Romania* (above) suggests as much. In any event, the line of authorities which includes *Leander, Amman* and *Rotaru* (para 7 above) supports the view that maintaining a file of personal information, using it and refusing access will often be a breach of the negative Article 8(2) obligation, not to interfere with private life.

34. It was argued by the defendants in *Ashcroft* that Article 8 was only engaged in *Leander* et al because they concerned a very specific context: secret surveillance and intelligence gathering by intelligence services. But in *Rotaru* much of the

information had in fact been gathered from the public domain. In both *Amman* and *Rotaru* the court emphasised that 'private life' has a meaning corresponding with the (very broad) meaning given to 'data' in the 1981 Data Protection Convention. And as the Court noted in *PG&JH v United Kingdom 25 December 2001 - Application 44787/98.*

> Private life considerations may arise however once *any systematic or permanent record comes into existence* of such material from the public domain. It is for this reason that files gathered by security services on a particular individual fall within the scope of Article 8 *even where the information has not been gathered by any intrusive or covert method* (see **Rotaru** "43-44)...

Unstructured government files: the unimplemented right of access

35. The amendments to the DPA made under ss68, 69 FoIA will give effect to a broader access right, in line with the approach just mentioned. In January 2005, DPA s1(1) will be amended to add a further class of information to the definition of data, namely

> (e) recorded information held by a public authority [which] does not fall within any of paragraphs (a) to (d)

This means that information that 'relates to' an individual, however recorded or filed by any public authority (as defined in FoIA s3) will be 'personal data' and *prima facie* accessible under DPA s7. So far so good.

36. However, a new DPA s9A will be added at the same time, limiting access to 'unstructured personal data' - which is, essentially, the data covered only by the new s1(1)(e). There are two controls

(1) For unstructured personal data, the SAR must contain 'a description of the data': s9A(2). This will avoid unstructured data falling within the scope of a 'trawling' SAR. But how precise does the description have to be? Clearly it cannot be right that the subject has to know what the substance of the information is. Presumably it would be enough to say something like:'the information on which the decision to refuse me a working peerage was based'?

(2) Secondly, there is a cost limit: if the estimated cost of providing the unstructured personal data goes beyond 'the appropriate limit', which is to be prescribed by the Lord Chancellor, the authority does not have to provide it (s9A(3)), though it may have to say yes or no whether it has any such data, if doing *that* is not too costly (s9A(4)). A measure of flexibility is built into the system; different amounts may be prescribed for different cases: s9A(5). But there is clearly the potential for dispute here. Suppose the limit is set low; a refusal to provide information on cost grounds might, depending on the nature and importance of the information at issue, engage

Article 8 and call for a proportionality test to be applied to the facts of the individual case. Alternatively, a wealthy and determined individual might perhaps try to cut this knot by offering to meet the costs involved from his own pocket.

12 January 2004