EVIDENCE TO THE JOINT COMMITTEE ON HUMAN RIGHTS CONCERNING THE INFORMATION SHARING PROVISIONS OF THE CORONERS AND JUSTICE BILL

Dr C. N. M. Pounder[1]
www.amberhawk.com
(January 2009)

1. Summary of content

This written evidence contains:

- A description of major concerns that arise from the information sharing provisions. I have limited myself to my "top ten"; but no doubt other points will be raised by others.

- An explanation as to why the provisions in the Coroners and Justice Bill will have the effect of degrading the protections afforded by the Data Protection Act and why the proposed Code of Practice is in conflict with ministerial policy objectives and therefore cannot afford protection to individuals.

- A solution that will improve individual protection and Parliamentary accountability whenever Information Sharing Orders are proposed. This solution is built round an explicit linkage between the Sixth Data Protection Principle and Article 8 of the ECHR.

- An Appendix that sets out more detail about the significant divergences between Thomas/Walport recommendations and the information sharing provisions in the Bill.

- An Appendix that describes the remoteness (arguably, the irrelevance) of the Code of Practice to the actual information sharing that could be legitimised in an Order.

***Note**: Clause 152 of the Coroners and Justice Bill ("the Bill") introduces a number of clauses into section 50 of the Data Protection Act (DPA) (clauses 50A-50F) and, correspondingly, clause 153 would introduce several changes to section 52 DPA. References in this submission to clauses (e.g. S.50A(1)) are references to the proposed changes to DPA.*

2. Top ten concerns about the information sharing provisions

I. **Lack of scrutiny.** There should be no need to remind the Committee of the number of times it has made comments about its inability to scrutinise wide-ranging statutory powers which impact on Article 8 ECHR, nor to refer to the omission of a human rights memorandum which would explain why the exercise of these powers is likely to be consistent with human rights

[1] *I have been working in data protection for more than twenty years and have given oral or written evidence to several Committees of both Houses of Parliament, including previous written evidence to the JCHR. All the historic evidence I have provided to the House is accessible from www.amberhawk.com*

legislation[2]. Once again, these very issues are presented to the Committee again in a heightened way by this Bill.

II. **The extension of information sharing beyond personal data**. The Bill extends information sharing by means of Statutory Instruments (SIs) well beyond what was explored in the Thomas/Walport report which limited its considerations to "personal data" sharing. The use of "any person" in S.50A(1) means the Bill applies to information sharing by any public or private body or individual. "Information sharing" powers are not limited to personal data (e.g. can apply the sharing of company confidential information)[3], and the person who receives the shared information might be a foreign government.

III. **The "exceptional" may become the routine**. Thomas/Walport recommended that the sharing of personal data should be legitimised in "*exceptional*" or *"precisely defined circumstances*"[4] and found that there was little evidence that the current laws do in fact prohibit necessary personal data sharing. Their recommended regime (to allow for *personal data sharing* in *"exceptional"* circumstances) has been replaced in the Bill by one that legitimises *"information sharing"* in *general* whenever it falls within "a relevant policy objective" (S.50F defines a "relevant policy objective" to be "a policy objective of that Minister"). Appendix 1 contains more detail on the divergences between the Bill's provisions and the actual Thomas/Walport recommendations.

IV. **The generality of an Information Sharing Order**. There is no limit as to how "*person*", "*purpose*" and "*information class*" are specified in an Order. There is no explicit requirement for the purpose of the information sharing to be one of those specified in Article 8(2) ECHR[5]. This contrasts with RIPA (Chapter 1, Part II which lists A.8(2) purposes explicitly).

V. **The prospect of unlimited data sharing from large Government databases**. The provision in S.50A(6) appears to be designed to facilitate data sharing from any Government database without Parliament being explicitly informed of this sharing when an Order is before Parliament. The prohibition in the clause *only* relates to Part 1 of RIPA, and specifies that RIPA must be identified in any Information Sharing Order if information sharing is to involve a RIPA-related database (e.g. the proposed national database of communications data). By implication, sharing from other national databases (e.g. the national identity register of the ID Card Act) does not need to be explicitly mentioned in an Order. This means that those data can be shared

---

[2] *See the Joint Committee on Human Rights (JCHR), 6th Report, Session 2007-8; Joint Committee on Human Rights (JCHR), 8th Report, Session 2004-5; Joint Committee on Human Rights (JCHR), 12th Report, Session 2004-5; Joint Committee on Human Rights (JCHR), 14th Report, Session 2007-8 and Joint Committee on Human Rights (JCHR), 16th Report, Appendix 20D, Session 2006-7 and Joint Committee on Human Rights (JCHR), 19th Report, Session 2004-5. Recommendations 59 and 60 of the Home Affairs Select Committee's report into ID Cards (session 2004/5); described powers in the ID Card Bill as "unacceptable", yet they exist in the ID Card Act 2006 in the same form.*

[3] *Thomas/Walport considered the sharing of "personal data"; the Bill concerns "information sharing" which extends beyond personal data.*

[4] *Paragraph 8.40 Thomas/Walport*

[5] *The Committee should look at the legal advice published in connection with data sharing associated with the Citizens Information Project (Annex 8 of http://www.gro.gov.uk/cip/Definition/FinalReportAnnexes/index.asp). This suggests that the powers are consistent with Human Rights obligations because they fall within the "margin of appreciation"*

from these other national databases by means of a general order-making provision. As there is no limit on the amount of personal data shared (and by whom), this prospect raises serious questions concerning the adequacy of Parliamentary scrutiny of public policy towards these national databases.

VI. **The exclusion of critical comment on the purpose of the processing**. Under S.50D(4) of the Bill the Commissioner writes a report on an Information Sharing Order, but he is not allowed to comment on whether "the sharing of information enabled by the order is necessary to secure a relevant policy objective" (as S.50D(4) excludes S.50A(4)(a) from the Commissioner's ability to make recommendations). The problem is that the "relevant policy objective" translates, in data protection terms, to the purpose of the processing of personal data, so the effect is to inhibit the Commissioner from commenting on the purpose of the processing. As most of the data protection principles[6] which it is the Commissioner's duty to enforce are directly or indirectly linked to the processing purpose, it is quite possible that the Commissioner's recommendations in relation to purpose could be ignored if the sharing proposed is "necessary to secure a relevant policy objective". This could also prevent him ruling on questions of necessity and proportionality in relation to particular activities, undertaken for that purpose. In addition, it is difficult to see how the Commissioner can report on matters outside his remit (e.g. when information sharing involves the disclosure of information that is not personal data).

VII. **The range of the powers**. The powers are widely drawn and their application is very broad (i.e. orders could require disclosure of information by law; power to demand information, power to override an obligation of confidence; power to modify the impact of the Data Protection Act itself; provide for offences for a failure to share). There is no explicit provision in the main sharing provisions which would facilitate data subject rights and freedoms (e.g. right to object to data sharing; need to obtain consent to sharing in most cases). Instead, these provisions can "modify" the application of any law (including the Data Protection and Human Rights Acts) which could inevitably weaken the protection afforded to data subjects.

VIII. **The lack of transparency**. There is no obligation to disclose to the Commissioner or Parliament any background document or legal advice about a proposed Information Sharing Order. There is no obligation to answer any formal request for information from the Commissioner. There is no obligation to engage the public on the subject of a draft Information Sharing Order. The Commissioner's first sight of a detailed proposal for information sharing could be a draft SI full of legal text and he could have only 21 days to respond. The Justice Committee has drawn this problem to the attention of the House[7].

IX. **The irrelevance of the Code of Practice.** There is nothing in these information sharing clauses which expressly states that the sharing of personal data has to be consistent with the Code of Practice. The Code is *not* the statutory code of practice envisaged by the Commissioner; rather it is just guidance on best practice. The Code is not subject to approval by Parliament; rather, it is subject to approval by the Secretary of State (SoS). There is no provision which sets out what

[6] *The word "purpose" is linked to all the Principles (except the Sixth Principle which deals with rights) either via the Principle, or its statutory Interpretation, or in Schedules 2-4 of the Act.*

[7] *The Report, Coroners and Justice Bill, is published as the Committee's Second Report of 2008-09, HC 185.*

happens if there is a disagreement between SoS and Commissioner about the content of a Code. There is no active role for Parliament in relation to the content of a Code. Appendix 2 contains more detail on the likely irrelevance of the Code to the actual information sharing.

X. **Orders can be implemented to achieve purely administrative objectives**. For example, suppose Ministers are told by civil servants that the problems associated with one of the Government's big database projects would be resolved if they used criminal convictions from the Police National Computer. The Bill allows the Minister to argue that the sharing was necessary to secure a policy objective, it was proportionate as there was no other way of securing the policy objective (abandoning a large IT project is not an option), and it was in the public interest to secure the policy objective (given the amount of money committed to the project). This means that sharing which could be excessive and disproportionate in terms of Article 8 becomes necessary and proportionate in terms of realising a policy objective[8].

3. How the proposed changes degrade the protection afforded by the Data Protection Act

Whenever government uses powers which affect the way in which the data protection principles apply to the processing (as in this Bill and other legislation), it follows that the safeguards for individuals *cannot* be safely grounded in the application of the Data Protection Act.

The first reason for this is that public sector data controllers can be placed in a different position when they are subject to legislation which require them to process data in specific ways. Whereas private sector data controllers, such as banks, must fit their processing around the obligations of the data protection principles, powers available to Ministers can change how the principles apply to public sector data controllers. These powers enable government, in a sense, to *fix* the data protection obligations so that they *fit* its processing objectives[9]. Specifically, once the processing of personal data is defined as lawful by an Information Sharing Order, then the fairness obligation under the first principle is largely avoided; processing is automatically justified under condition 3 or 5 of schedule 2; processing automatically satisfies the lawfulness requirement of principle 2 and application of some of the other principles may also be affected (see footnote). Obviously the ICO cannot enforce these principles as if they were unmodified by the order.

I am not convinced that a Code of Practice and related provisions can afford the necessary protection. I have already commented that there is nothing in Bill which expressly states that the sharing of personal data has to be consistent with the Code of Practice; that the Code is not the statutory code of practice envisaged by the Commissioner, that it is not approved by Parliament and is subject to SoS approval only. Even if these issues were resolved, the Code of Practice cannot possibly "trump" an

[8] *The Bill uses the phrase "necessary to secure a policy objective", and this might be different to the requirement that any interference is a "necessary" interference with private and family life as required by A.8(2) of Human Rights. Similarly, because "proportionate to that policy objective" is used in S.50(4)(A) the Bill, this might be different to the requirement that any interference with private and family life is a "proportionate" interference (as required by A.8(2) of Human Rights law*)

[9] *Section 12 of the Children Act 2004, for example, provides Ministers with powers which can apply to the content of personal data stored on a database as well as accuracy, security, retention, management, disclosure and access. Such powers dictate how the data protection principles apply in practice – for example if the powers were used to define a 10 year retention period, then even if the ICO takes the view that this is excessive and unnecessary he is not going to be able to enforce the Third and Fifth Principles so as to require deletion of personal data after a shorter period.*

order if that order defines the lawful purpose(s), the items of the personal data involved, retention times, and any onward disclosure.

However, my main objection to the Code is perhaps more fundamental. If one accepts that Ministers must be free to determine policy (i.e. to define the processing purpose which realises the policy objectives), then it is not possible to give the Commissioner control over a Code of Practice that describes how the data protection principles apply to that processing purpose. As most principles link to the purpose of the processing, any enforcement of the principles by the Commissioner necessarily involves a conflict with ministerial policy objectives.

This creates a dilemma. The more remote the Code is from the actual processing, the more it is an irrelevance if it is intended to protect data subjects. The closer it is to the processing, then more it is a barrier to Ministers achieving their policy objectives. The Bill's approach to this dilemma is to define a Code of Practice that is remote from the processing of personal data (see Appendix 2 for detail) with the result that it affords little protection.

Finally, consider the case in which a data subject asks the ICO for an assessment where he thinks his personal data should not have been shared. The Commissioner would be judging a complaint in the context of his own decision to approve the Code and/or his tacit approval of the order. The complainant could well see this as a compromised or flawed procedure.

4. There is a solution to improve individual protection and Parliamentary accountability

The Information Sharing Order procedure identified in this Bill will (inappropriately in my view) determine matters of significant public policy by use of secondary legislation that is not sufficiently scrutinised by Parliament. As these Orders potentially concern personal data relating to every UK citizen, any mistake in policy objectives risks further undermining the respect the public has for Parliament and for the political process in general.

If Ministers continue to overlook Parliamentary recommendations to the extent identified previously[10] in the context of use of expansive powers which cannot be effectively scrutinised, it is likely they can choose to disregard any ICO report into which raises concerns about an Information Sharing Order. As happened in the case of the ID Card Bill, the Secretary of State (SoS) could dismiss any critical report coming from the Commissioner as merely a report from a body opposing the measure[11].

I think that there is fairly simple solution which would improve Parliamentary scrutiny of order-making powers, protect the individual from excessive use of powers, and would not interfere with Ministerial policymaking. This solution starts with the recognition that any personal data sharing is an interference with private and family life. It follows that:

- all data sharing without consent of the data subject must be for a purpose identified in Article 8(2) (i.e. crime, national security etc.), and

[10] *See reference 2*

[11] *In the context of the ID Card, the then Home Secretary (Charles Clarke) dismissed the Information Commissioner's concerns as he was "a long-standing opponent of the identity card system" (28 Jun 2005: Column 1157*).

- all other data sharing (i.e. not falling within an Article 8(2) purpose) should be under the control of the individual concerned (there would either be consent to the data sharing or a right to object).

The solution has three components:

1. A linkage between Article 8 ECHR and DPA via the Sixth Data Protection Principle (dealing with rights of data subjects).

2. A new power of the Commissioner to challenge an Information Sharing Order (or any order under other legislation which requires the processing of personal data) on the grounds that the Order is inconsistent with Article 8.

3. An enhanced right to object to the information sharing in circumstances where the sharing is not for a purpose identified in Article 8(2).

Commentary on component 1: linkage between data protection and human rights

The linkage between the human rights and data protection regime would be created by the sixth data protection principle, if it were to be redrafted in the following form:

> *"Personal data shall be processed in accordance with the rights of data subjects under this Act and, in particular, personal data shall be processed for a lawful purpose that respects the private and family life or correspondence of each data subject".*

The interpretation of this principle has to be qualified in a way that engages the exemptions found in Article 8(2) (i.e. provide suitable exemptions for national security, law enforcement etc). In addition, by implementing a privacy right limited to the processing of personal data under the auspices of the Data Protection Act, the processing of personal data for the Special Purpose (i.e. freedom of expression purposes) will be left undisturbed[12]; so investigative journalism, for example, would be unaffected by the change.

Commentary on component 2: Powers to enforce the linkage

The Commissioner would need powers to enforce the linkage between the two regimes. One way would be for him to be empowered to serve an "Article 8 Incompatibility Notice" which could be applied, for example, in the case of the use of Ministerial powers which have been generously interpreted.

An "Article 8 Incompatibility Notice" would be intended as a last resort power to be used where necessary to test whether a particular SI or element of primary legislation is compatible with human rights law[13]. This notice could be appealed to the Courts by the Secretary of State so that the issue of compatibility of an SI can be challenged within the framework provided by existing human rights law,

[12] *Section 32 exemption disapplies most of the DPA (including the Sixth Principle) until publication of the personal data concerned.*

[13] *This ability should apply, for example, if powers relating to the use of Section 22(2)(h) of the Regulation of Investigatory Powers Act 2000 (access to communications data "for any purpose…….specified for the purposes of this subsection by an order made by the Secretary of State") were used in a way that other Commissioner found to be excessive.*

and can be tested via the Courts. Unlike the Code of Practice, this linkage does *not* create an interference with a Minister's policy-making ability – it would be a last-resort safeguard to ensure that any Order which legitimises an interference (i.e. the sharing of personal data) is consistent with A.8(2).

My own view is that such a notice would work in the same way that the nuclear deterrent works – civil servants and Ministers would not want to take the risk of a notice being served. So the mere fact that the Commissioner could challenge an order on the basis of incompatibility with A.8 would ensure that Civil Servants and Ministers will be consulting the Commissioner (and providing full information) before finalising any proposed order. It would be analogous (but in reverse) with the provision (at s.53 FOIA) for ministerial override of an ICO requirement of government to release information under the Freedom of Information Act. The Commissioner has enough powers to engage with Parliament and the public if that is what is needed.

If the ICO issued such a notice it would signal a serious dispute between government and the Commissioner and one would expect a Parliamentary Committee to investigate. In fact, as a condition precedent to serving a notice, the Commissioner could be required to report to a Parliamentary Committee that a particular use of ministerial powers or procedure should be reviewed. Alternatively the Commissioner could be required to negotiate with the Minister before serving a notice and/or to report to Parliament. In other words, the existence of an "Article 8 Incompatibility Notice" could facilitate the badly-needed informed public and Parliamentary debate on any information sharing policy (and reassure the JCHR that ministers are accountable for the exercise of their powers).

It is recognised that an Article 8 Incompatibility Notice could be seen as politicising the ICO. However, the ICO has recommended that the current single Commissioner should be replaced by a multi-member Commission and this change should ensure that any Notice could only be served with the full support of that multi-member Commission. In addition, the existence of this Notice would make it difficult for the ICO to report to a Secretary of State for Justice – that is why the recommendation of the Justice Committee that the ICO should be funded directly by Parliament (and report to Parliament) should be supported[14].

Commentary on component 3: an enhanced right to object

The Section 10 DPA right to object to processing of personal data currently requires that the processing is causing or would cause substantial unwarranted damage or substantial unwarranted distress. Additionally, the right is restricted to processing undertaken in limited circumstances[15], so it is very difficult in practice to exercise, which means that it is rarely used by data subjects.

I propose that the S.10 right be changed so that where the processing objected to is personal data sharing carried out in circumstances which are not justified by reference to the purposes specified in Article 8(2), this right operates as easily as the right to object to the processing of personal data for a direct marketing purpose. In other words there would in these circumstances be no requirement of damage or distress, substantial or otherwise, nor would the onus be on the data subject to show that the processing was unwarranted, and in addition, the right would have to be exercisable when the

[14] *See reference 7*

[15] *The processing has to be legitimised in terms of paragraph 5 and 6 of Schedule 2 of the DPA*

Schedule 2 ground for processing was condition 3 – legal obligation, not just conditions 5 & 6 as at present. Since the processing purpose does not need to be concealed from the data subject, it would be appropriate to offer the right to object in a fair processing notice informing the data subject of the purpose of the processing. In this way, individual choices concerning data sharing can be exercised via the familiar opt-in or opt-out arrangements as used in direct marketing.

Such a revised right to object would not interfere with processing of personal data for powerful public interest purposes, such as crime prevention, but would arise where data sharing is undertaken merely for purposes of administrative convenience[16]. Of course, it follows that if individuals trust the data sharing arrangements undertaken by public authorities in these circumstances, then it is unlikely that they would ever need to exercise the right to object.

The information sharing orders of this Bill do not allow much if any opportunity to object to data sharing and requires the public to trust whatever the public authority says are its data sharing requirements. It should, in my view, be replaced by a mechanism which requires the public authority to earn the trust of the public it serves if it wants to engage in the sharing of personal data for non-Article 8(2) purposes.

Concluding comment

My hope is that the Committee will recommend that these ideas are explored in order to see whether it (or something which would deliver similar safeguards) provides a politically viable and legally consistent framework that balances the divergent interests of Ministerial policy objectives, Parliamentary accountability and protection of individuals.

[16] *Section 1(4) of the ID Card Act allows for such data sharing on "efficiency" grounds. The right to object would apply to this purpose but not, for example, to the crime related purpose.*

Dr. C. N. M. Pounder, www.amberhawk.com, chris.pounder@amberhawk.com

APPENDIX 1: More detail on the significant divergences from Thomas/Walport recommendations

(a) **"Recommendation 7(a):** We recommend that new primary legislation should place a statutory duty on the Information Commissioner to publish (after consultation) and periodically update a data-sharing code of practice. This should set the benchmark for guidance standards"

A. Commentary on Recommendation 7(a):

Thomas/Walport clearly envisage "A statutory code of practice"... that " would establish a central reference point from which further, more consistent guidance could be derived" and "We consider it vital to provide that the general code is laid before – and approved by – Parliament"[17].

The model for such a Code would be on the lines of Section 67 of the Police and Criminal Evidence Act 1984 where there is an SI which Parliament has to approve in order to activate the Code. Instead actual model for the Code in the Bill is provided by the Section 38 of the Road Traffic Act 1988 in relation to the Highway Code; here the Code is approved by the Secretary of State and laid before Parliament.

As the Code is for best practice guidance, approved by the Secretary of State, there might not be any Parliamentary debate re the Code, or any related benchmarking/other guidance. The Code only covers personal data whereas the sharing provisions relate to any information.

(b) "**Recommendation 7(b):** We further recommend that the legislation should provide for the Commissioner to endorse context-specific guidance that elaborates the general code in a consistent way".

B. Commentary Recommendation 7(b):

Thomas Walport envisage the Commissioner having a role to modify the Code so that it impacts on the Order that allowed the data sharing. This recommendation has not been implemented. The Commissioner's involvement depends now on use of Information Commissioner's powers and these will have limited effect if the Order has modified the impact of the Principles on the processing.

(c) **"Recommendation 8(a):** We recommend that where there is a genuine case for removing or modifying an existing legal barrier to data sharing, a new statutory fast-track procedure should be created. Primary legislation should provide the Secretary of State, in precisely defined circumstances, with a power by Order, subject to the affirmative resolution procedure in both Houses, to remove or modify any legal barrier to data sharing by:

- repealing or amending other primary legislation;
- changing any other rule of law (for example, the application of the common law of confidentiality to defined circumstances); or
- creating a new power to share information where that power is currently absent".

[17] *Paragraphs 8.33 and 8.34 of Thomas Walport*

C. Commentary on Recommendation 8(a):

Thomas/Walport see these powers as occasional and based on the circumstances (that the Commissioner can test through application of his Code of Practice and statutory endorsement of context-specific guidance). The report states "Although we found the most significant barrier or hindrance to effective data sharing to be legal uncertainty and confusion, ***there are occasions*** when real legal obstacles – either statutory or common law prohibitions, or the absence of the necessary legal power – inhibit the sharing of data" (my emphasis; Para 8:40).

Thomas/ Walport add: "When making an Order, the Secretary of State could include necessary conditions and safeguards, addressing in particular any concerns of the Information Commissioner. And because of its ***exceptional and potentially controversial nature***, the Order would be subject to the affirmative resolution procedure". (My emphasis; Para 8:40).

Government Implementation: the "exceptional" or **"**precisely defined circumstances" of the Thomas/Walport Recommendations are satisfied if they fall within any general "policy objective" of a Minister. Because the Code of Practice is not linked to the information sharing Order, there is no guarantee that the Information Commissioner's concerns will be addressed. In addition, it is difficult to see how the Commissioner can provide guidance on those matters that do not involve personal data

i. **Recommendation 8(b):** "We recommend that, before the Secretary of State lays any draft Order before each House of Parliament, it should be necessary to obtain an opinion from the Information Commissioner as to the compatibility of the proposed sharing arrangement with data protection requirements. There should be a requirement that a full and detailed privacy impact assessment would be published alongside any application, to assist both the Information Commissioner and Parliament's consideration".

ii. **Recommendation 8(b):** Thomas Walport say that "we believe this process would not be appropriate for large-scale data-sharing initiatives that would constitute very significant changes to public policy, such as those relating to the National Identity Register or the National DNA database " (para 8.47)

D. Commentary on Recommendations 8(b):

Re Government Implementation of (i) : In his assessment of the arrangements, the Commissioner cannot report on the purpose of the processing. There is no explicit requirement for a Privacy Impact Assessment. Publishing details in relation to an Order do not relate to the detail of draft Order but on the principle of whether an Order is desirable. The Commissioner has 21 days to respond to a draft Order that may contain pages of legal text.

Government Implementation of (ii): An information-sharing order may not enable any sharing of information which would be prohibited by Part 1 of the Regulation of Investigatory Powers Act 2000 without the RIPA provision being explicitly identified. This implicitly allows large-scale data-sharing initiatives involving other databases do not need to be explicitly identified.

APPENDIX 2: The remoteness of the Code of Practice to the actual information sharing

The data protection issues associated with the sharing of personal data will arise **following** the implementation of an Order **after** it has been passed by a Parliamentary procedure that affords little scrutiny. This means that the following stages, although important in themselves, can be remote from the actual problem encountered by a data subject after his personal data have been shared. These stages are:

(a) **Production of a Code of Practice on the sharing of personal data**. This Code is limited to personal data and not information sharing in general and cannot cover all the privacy issues (e.g. sharing personal details from privately held, moderately structured manual files; commercial privacy). It is therefore incomplete. This document is also likely to contain high level principles or the overall best practice guidance that need to be applied **when the content of the Order is being produced**. As such its relevance to the problems encountered by data subjects who don't want the personal data to be shared could be very limited.

(b) **Debate about a policy objective**. Ministers choose who and how they want to contact re the policy; the Information Commissioner can choose to respond if need be. Debate can be condensed into a relatively time period. As public policy debate centres on how best the public interest is served (e.g. the general benefit to the greatest number), its relevance to the actual processing problem encountered by a minority of data subjects could be limited.

(c) **Production of a draft Order for the Commissioner to consider**. There is no public debate on the detail of a draft Order. The Commissioner has 21 days to work out what is intended and is excluded from considering the purpose of the processing – yet it is the purpose of the processing that gives meaning to the data protection principles[18]. The Commissioner is not provided powers to demand any information he might need (legal advice on human rights obtained by the Government).

(d) **Enactment of the draft order by Statutory Instrument (SI).** The SI procedures of Parliament is limited and any debate will focus on the policy and generalities associated with the policy objective of the protection of individuals in general. This also is likely to be remote from the actual processing problem encountered by data subjects.

(e) **Processing of personal data legitimised by the Order**. Government Departments will then interpret the Order and put it into practice.

The recognition of any data protection issue comes **AFTER** stages (a) to (d). At this stage if data subjects are adversely affected by the processing, it is unlikely that a breach of a data protection principle has occurred. This is because the powers in the Order have modified the impact of most Principles so that the complained-about processing is lawful (e.g. the Order may define the purpose of the sharing, its legal basis; legal recipients or third parties; what they can do with the personal data; for how long and what is disclosed).

Of course if there is a procedural failure (e.g. something like HMRC's lost disks; failure to share accurate records), then the Commissioner can assist the data subject. However, he will be unable to enforce the data protection principles that relate to the purpose of the sharing itself, as the Order makes that processing purpose lawful.

Finally, the complaint will be to a Commissioner who is judging the complaint in the context of his own Code of Practice and/or his tacit approval of the Order. The complainant could well see this as a compromised or flawed procedure.

[18] *See the discussion associated with references 8 and 9.*