



Information Commissioner's Office

Promoting public access to official information
and protecting your personal information

Andrew Dismore MP
Chair, Joint Committee on Human Rights
House of Commons
7 Millbank
London
SW1P 3JA

27 February 2009

Dear Mr Dismore

Coroners and Justice Bill: Information Commissioner's response to the Joint Committee on Human Rights.

Thank you for your letter of 23 February 2009, inviting our comments on a number of questions about the data protection proposals in the Coroners and Justice Bill that you have raised with the Secretary of State for Justice.

The data protection provisions of the Coroners and Justice Bill present a welcome but long-overdue opportunity to put rigorous safeguards in place and to address long-standing deficiencies in the Information Commissioner's powers, such as those you identified in last year's report on Data Protection and Human Rights. However, the Bill needs to be improved if it is to make the regulation of personal information more effective, and ultimately to help safeguard individuals' right to respect for their private life. Wider use of personal data must be balanced by the inspection and information gathering powers for the Information Commissioner's Office which will actually work in practice. The Bill's information-sharing provisions are too wide and the safeguards relatively weak. As it stands, we regret that the Bill will not give us powers to ensure that all those processing personal information do so in compliance with the principles of data protection. In particular, we must be able to serve an Assessment Notice on *any* data controller and there must be meaningful sanctions for ignoring a Notice. We received welcome new powers in the Criminal Justice and Immigration Act 2008 to levy fines on data controllers for deliberately or recklessly breaching the data protection principles. However it is important that the Government brings these powers into force as soon as possible. Effective safeguards and sanctions are vital if we are to "reap the benefits of data sharing, where it is considered desirable, without calling into question the right of ordinary people for respect for their personal lives." (JCRH Report on Data Protection and Human Rights)

Our responses to your questions follow:

JCHR V1.0 27-2-09

38. Does the Government accept that a breach of Article 8 ECHR could arise as a result of the failure of a private individual or a company to comply with the data protection principles.

• If not, why not?

• If so, does the Government accept that greater scrutiny of the private sector by the ICO would reduce the risk that such a breach could arise?

The right to respect for private life in Article 8 ECHR imposes a positive obligation on the State to ensure that its laws provide adequate protection against the unnecessary processing of an individual's personal data. This is recognised in EU Data Protection Directive 95/46/EC, from which the DPA derives, which specifically states that "the object of the national laws on the processing of personal data is to protect the fundamental rights and freedoms, notably the right to privacy, which is recognised...in Article 8...".

The processing of personal data including its collection, retention, disclosure and sharing amounts to interference with an individual's rights to respect for his or her privacy. Article 8 ECHR does not prevent this, but it does require that if this interference is to take place, then certain safeguards for individuals would have to be provided. Whilst the duty to have respect for private and family life is very high-level, neither the Human Rights Act 2000 nor the ECHR itself provide any practical guidance on how to act in a way that ensures that the individual's right to respect for his or her private life.

The DPA provides this practical guidance through a set of principles of good practice for the handling of personal data. The principles require that any sharing of personal data is necessary and that any information shared is relevant, not excessive and kept securely. These principles apply to all data controllers without distinction as to whether they are in the public or private sector and provide a practical framework for balancing the need for data controllers to make the best use of the personal information they hold whilst respecting the individuals' private lives. In this way the protections afforded to the individual under Article 8 apply (through the DPA and its principles) to the handling of his or her personal information by any data controller whether public or private. The application of the DPA to private and third sector organisations is one of its strengths, given the enormous amount of sensitive and potentially damaging personal information held outside the public sector.

ICO certainly accepts that effective powers to scrutinise the private sector would reduce the risk of breaches arising. An assessment notice – provided for by clause 151 of the Bill - will allow us to inspect an organisation to determine whether it is complying with the data protection principles. However, as it stands, the Bill will only allow the ICO to serve an assessment notice on a government department or a designated public authority. Given that these public authorities have to be designated by order it is not even clear how far into the public sector

our power will ultimately reach. The Bill would not allow the ICO to serve an assessment notice on a private or third sector organisation. We are strongly of the view that if individuals are to be protected properly, ICO must be able to serve assessment notices on all data controllers – including private sector, public sector and third sector organisations.

It is also difficult to understand why the Bill does not provide for any sanction if an assessment notice isn't complied with and yet does provide for a formal right of appeal against a notice. In order to make ICO's power of inspection effective, and to ensure the credibility of the inspection process, even if it is limited to public bodies, there must be a sanction where an organisation fails to comply with an assessment notice. One approach would be to introduce a clause similar to s.54 of the Freedom of Information Act 2000. This treats failures by public authorities to comply with our FOI notices as a contempt of court. Alternatively, failure to comply with an Assessment Notice could be taken as grounds to apply for a search warrant.

39. I would be grateful if you could explain why the Government consider it would be appropriate to subject any and all types of information to wider information sharing by ISO. For example, are there any reasons why the Government considers that the Bill should not be amended to exclude, for example:

- **information which would otherwise be protected as “sensitive personal data” for the purposes of the DPA 1998;**
- **medical records or medical or clinical information (other than anonymous patient data from which no patient can be identified);**
- **information held on the National DNA Database and other samples held by the police or others for the purposes of criminal investigation;**
- **information held on the national children’s database created pursuant to the Children Act 2004;**
- **records of criminal allegations or accusations;**
- **information held or gathered pursuant to the Safeguarding Vulnerable Groups Act 2006 (express provisions for information sharing for the purposes of safeguarding children and vulnerable groups are already provided on the face of that Act)?**

We fully accept that certain types of information are of particular sensitivity. This must be reflected in the way such information is collected, used and shared. However, we are sceptical about categorising certain types of information as sensitive and excluding these from the legislation’s Information Sharing Order provisions. There is a risk in attempting to define sensitivity exclusively according to information type. Context and the circumstances of the people the information is about must also be taken into account. For example, the mere name and address of a person on a witness protection scheme or escaping an abusive

partner would be of exceptional sensitivity and would need to be treated with particular care.

The (DPA) divides personal data into sensitive and non-sensitive types. The law provides for additional restrictions on the processing of sensitive information. However, we are not convinced that this distinction has worked well in practice. Part of the problem is the definition of 'sensitive personal data'. This includes trades union membership, but excludes financial information, for example. In general, we favour a risk-based approach to compliance that applies to all personal information, rather than an inevitably simplistic categorisation of personal information into sensitive and non-sensitive types. There is a danger that the problems we have encountered in the context of the DPA could re-emerge in the Coroners and Justice Bill. There would be particular confusion if the DPA were to be amended to include a definition of sensitive information in the context of ISO's that is different from the main DPA definition.

Information Sharing Orders should facilitate reasonable information sharing. In our opinion the sharing of even sensitive information could be reasonable, provided that it is proportionate, in the public interest and subject to rigorous safeguards. For example, information on communicable diseases is already shared in the interests of public health. We need to consider carefully whether it is desirable that the sharing of sensitive information, however that is defined, be entirely excluded from the Bill's Information Sharing Order provisions.

40. Does the Government consider that the power to modify any enactment, by ISO, includes the power to modify or disapply the provisions of the HRA 1998, including the Section 6 duty to act in a manner compatible with Convention rights?

This is for the government to answer. However, when the Thomas / Walport Data Sharing Review (DSR) recommended a fast-track procedure for removing or modifying a legal barrier to information sharing, it was certainly not the intention that it should be used to disapply the provisions of the Human Rights Act 1998 or the DPA.

41. Does the Government consider that this provision would prevent an individual from making a claim, under the HRA 1998, that the treatment of his or her personal information, despite being authorised by the ISO, had led to a breach of his or her right to respect for personal information (Article 8 ECHR)?

42. If so, why shouldn't the Bill be amended to include a savings clause similar to that inserted in the Civil Contingencies Act 2006, in order to provide a guarantee that individual public authorities processing information pursuant to an ISO will be subject to the requirement to act in a manner compatible with Article 8 ECHR?

43. I would be grateful if you could confirm that once information has been processed in accordance with an ISO, the final data controller of any personal data must hold and process it in a manner which is compatible with the Data Protection Act (DPA) 1998.

It has always been our understanding that the DPA would still apply to the processing of personal information carried out under an ISO. Nevertheless, we would welcome the introduction of a savings clause stating explicitly that the provisions of the DPA and HRA still apply when information is shared under an ISO. For example, s.68 (4) of the Serious Crime Act 2007 explicitly states that nothing in its disclosure of information provisions authorises any disclosure which contravenes the DPA.

44. Is there anything in the Bill which would prevent the Government proposing the permanent amendment or modification of the DPA 1998?

The wording of clause 152 is very wide. There is nothing in it that would prevent the DPA being amended. It says that an information order may “modify any enactment” or “remove or modify any prohibition or restriction imposed (whether by virtue of an enactment or otherwise) on the sharing of the information by that person or on further or onward disclosure of the information”. The intention of the DSR recommendation was to provide a means for overcoming essentially technical barriers to reasonable information sharing. It was certainly not intended that information-sharing should be facilitated by weakening data protection safeguards. Indeed a major theme of the DSR was that data protection safeguards need to be made more effective as a counter-balance to greater information sharing.

The UK’s data protection legislation implements the European data protection directive (95/46/EC). The UK could well fall foul of its international obligations if it amends or modifies the DPA in such a way that the protection of individuals is undermined.

45. I would be grateful if you could provide a fuller explanation of the Government’s view that the test for an ISO is appropriately defined. In particular:

- **Please explain why the Government considers it appropriate to link the making of an ISO with an individual Ministerial policy? Are there significant reasons why the Bill should not be amended to limit information shared under ISO to information which is necessary to meet the public functions of the Minister or any other public authority exercising public functions?**
- **Why should the Bill not be amended to link the making of an ISO more closely to the legitimate aims identified in Article 8(2) ECHR?**

We do think that the scope for making an ISO should be narrowed to bring it into line with the relevant DSR recommendation. This said 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.*”

We are not convinced that amending the wording of clause 152 to link the making of an ISO to Ministerial public functions would significantly improve safeguards. We had thought it implicit that securing a relevant policy objective would be part of a Minister’s public functions. We find it difficult to envisage making an ISO for non-public purposes.

An appropriately worded savings clause – see question 43 above – would make it clear that ECHR tests also need to be satisfied when an ISO is made.

46. I would be grateful if you could confirm whether the Minister proposing an ISO would be required to make a Privacy Impact Assessment of the proposed Order and whether (a) that assessment would be made available to the Information Commissioner together with the draft Order and (b) it would be published to assist wider public scrutiny?

The responsible Secretary of State will have an important role in terms of putting safeguards in place as a precursor to granting consent for an ISO. The MoJ’s Memorandum to the House of Lords Delegated Powers and Regulatory Reform Committee says that a Privacy Impact Assessment (PIA) will be required for all proposed information-sharing orders. The Secretary of State’s role and the relevant safeguards should be specified on the face of the Bill.

We would expect the PIA to be made available to us – this would be extremely helpful to us in preparing our report. Ideally this would happen early in the process, providing an opportunity for a draft ISO to be amended, or modified, prior to the ‘formal’ 21 day reporting period beginning. We would also expect the PIA to be published. This should form a key element of the scrutiny process.

47. Does the Government accept that, under the proposals in the Bill, the report of the Information Commissioner can have little effect, other than to inform public and parliamentary opinion?

- **If not, what will be the practical effect of a negative report of the Information Commissioner?**
- **If you agree, wouldn’t it be more appropriate to allow the Information Commissioner to report on the proposal for the ISO in any terms that fall within his remit, including commentary on the necessity for the ISO and its implications for the right to respect for personal information?**

We had understood ICO's role here as being to provide evidence to Parliament, to help it to inform its decision as to whether to approve an ISO. Of course it is, quite rightly, Parliament's prerogative to pass an ISO in the light of an unfavourable ICO report. It is difficult to envisage how the ICO's role could be strengthened here without undermining the affirmative resolution process; it would clearly be impossible, and undesirable, for there to be any compulsion for Parliament to agree with the ICO's conclusions. It would, of course, be open to the ICO to then take regulatory action against the organisations involved in an information-sharing initiative that breaches the DPA. However, we do think that it would be brave for government to bring a proposal for an ISO forward in the face of an unfavourable ICO report.

The amended s.50(D)(4) of the DPA would only allow the ICO to report on whether the effect of the provision made by the Order is proportionate to the policy objective, and whether it strikes a fair balance between the public interest and the interests of any person affected by it. The ICO may not report on whether the sharing of information enabled by the Order is necessary to secure a relevant policy objective. This touches on a difficult tension between the informational consequences of a policy objective and the policy objective itself. Inevitably the two are inseparably linked. We do think that must fall to the Minister, rather than to the ICO, to set the policy objective. However, we think it entirely right that ICO should be able to comment on whether the proposed information sharing is a necessary and proportionate means of achieving the policy objective.

There will be inevitable overlap between the three limbs of s.50A(4), and consequent difficulty in determining the extent of the ICO's reporting role. We believe, therefore, that ICO's role could be made clearer and more effective if the Information Commissioner were additionally, or alternatively, able to report more generally on compliance with the data protection principles. This would allow ICO to make a more rounded and comprehensive assessment of an information sharing proposal, including, for example, the relevant security arrangements. This would require amendment of clause 50D(4).

Please let me know if you require any further information or assistance.

Yours sincerely

Richard Thomas
Information Commissioner