



Privacy International

Black Zone Report Series

Report on the UK Data Sharing Legislation

SHARING THE MISERY

**The UK's strategy to circumvent data privacy
protections**

January 2009

About Privacy International

Privacy International (PI) is a human rights group formed in 1990 as a watchdog on surveillance and privacy invasions by governments and corporations. PI is based in London, England, and has an office in Washington, D.C. The organisation has been at the forefront of privacy issues worldwide for two decades and has conducted dozens of investigations, compiled numerous reports and provided testimony to parliaments throughout the world.

According to our Memorandum of Association, PI's objectives are:

- To raise awareness of and to provide education about threats to personal privacy;
- To work at a national and international level toward the provision of strong and effective privacy law;
- To monitor the nature, effectiveness and extent of measures to protect privacy and personal data;
- To conduct research into threats to personal privacy;
- To monitor and report on surveillance activities of security forces and intelligence agencies;
- To scrutinise the nature, extent and implications of transborder flows of information;
- To engage in advocacy at a national and international level such as making representations to bodies such as the United Nations, the Council of Europe and the OECD;
- To seek ways through which information technology can be used in the protection of privacy.

PI now has active associates and networks in over 40 countries. It is registered in the UK as a non-profit private limited company (no. 4354366).

PI is advised by an 82 member international advisory board and is overseen by a board of seven distinguished UK-based trustees.

www.privacyinternational.org

privacyint@privacy.org

Introduction

Of the hundreds of issues engaged each year by Privacy International, a small handful stand out because of the fundamental risk they pose to the foundations of privacy protection.

In January 2007, Privacy International decided to initiate the “Black Zone” report series. These reports will deal with issues that we regard as constituting an exceptional danger to privacy.¹

The UK government’s proposal to legislate for wide scale sharing of personal data is one such instance, and internationally is the first occasion in recent months that we have seen an example of risk at such a fundamental level. The scale of the danger to privacy should be seen in the light of other current UK proposals, such as mass communications data surveillance and nationwide vehicle surveillance. These latter projects constitute a major threat, but do not encompass the breadth or potential corrosive effect on existing protections.

The mass exchange of personal information has the potential to deliver some benefit, however it also presents vast risks associated with governance, privacy, security and human autonomy. In the rush to institute data sharing, these aspects have largely been ignored.

Privacy International took the decision to prepare this report on the basis both of the dangers inherent in current legislative proposals and the unprecedented way in which they have been created.

The aim of this report is to bring to the attention of the public, Parliament and media the urgent need to consider the extraordinary dangers created by the proposal. Previously people’s consent was required, but now the consent of the governed is not longer being sought. In fact, the Government’s proposal eradicates *consent* from the governing framework, thus placing not only our data at risk but also fundamental tenets of our democracy.

¹ For instance, in 2007 we published reports on the risks to journalists and a free media presented by government surveillance programmes. In 2008 we focussed on the risks of the UK Government DNA database and how it could act as a model to other governments, and governments’ ambiguous claims of ‘national security’ to justify wide-scale access to personal data.

Summary of key points

The information sharing provisions in the *Coroners and Justice Bill* constitute the gravest threat to data protection in the 25-year history of the Data Protection Act, and are among the most wide-ranging and potentially intrusive proposals ever laid before Parliament.

Clause 152 of the Bill will permit an almost limitless range of data sharing opportunities both within government and between commercial organisations, including, but not limited to:

- Provision without patient consent of NHS files to medical research organisations;²
- Massive expansion of the national DNA database, including for purposes other than the detection of crime;³
- Bulk provision of NHS and other medical files to the insurance industry;⁴
- Disclosure of police intelligence data to private investigators and investigation departments of companies;
- Bulk transfer of personal financial data to HMRC and other government departments;⁵
- Disclosure of all vehicle insurance data from insurance companies to DVLA;⁶
- The sharing of client and customer lists between companies and with the government⁷ including, e.g. harvesting of biometrics by indirect means such as from 'Clubscan' databases, under pressure from licensing authorities;

² These provisions are already in place in statute. S.60 of the Health and Social Care Act 2001 transfers control over disclosure of patient data to the Secretary of State: "The Secretary of State may by regulations make such provision for and in connection with requiring or regulating the processing of prescribed patient information for medical purposes as he considers necessary or expedient".

³ This vision was endorsed by the 2003 White Paper on Genetics, which also proposed genome screening every baby in the NHS at birth. The proposal was rejected by the Human Genetics Commission, but is due to be revisited in 2010.

⁴ Health and Social Care Act, s.60

⁵ 'Anti-fraud body to further trawl civil servants' bank data', Tom Young, Computing, December 11, 2008.

⁶ From 2009 the Department of Transport's Continuous Insurance Enforcement programme will permit the DVLA's vehicle register to be compared with the Motor Insurance Bureau's database

⁷ 'Environment Agency takes phishing rather too literally?', Toby Stevens, Computing Weekly, April 21, 2008.

- Routine sharing of information from government departments to the intelligence and security services, without parliamentary approval, and vice versa (currently now forbidden);⁸
- Transfer of UK police data to foreign police agencies in Europe and elsewhere;⁹
- Disclosure of police records to social services and children's data systems, and vice versa;
- Disclosure of Automated Numberplate Recognition data to the Highways agency and other organisations;¹⁰
- Access by Criminal Records Bureau to police intelligence data, and an Information Sharing Order could also permit employers to share CRB check data;
- Full disclosure of telecommunications data from service providers to government;¹¹
- Automatic population of the National Identity Register with, e.g. complete electoral roll and tax records (effectively, near-universal registration without consent);¹²
- Sharing of data between council tax records and national databases including the electoral roll¹³, and between national databases to councils for collecting council tax;¹⁴
- Bulk disclosure of hotel registration data to police and HMRC.
- In the context of anti-prostitution policy, STD clinic data to be shared with the government;
- Routine transfer of background data of air travellers to destination countries¹⁵, but also to benefits authorities and HMRC – or DCSF to track down people taking their children to Disneyland in term time;

⁸ 'Spooks 'to share terror secrets'', BBC News Online, May 29, 2003.

⁹ This process is mandated in the EU's Prum Convention but ideally would have UK statutory footing.

¹⁰ This type of disclosure is generally prohibited because of ACPO guidelines, but a precedent exemption was given in January 2009 to Oxfordshire police.

¹¹ This is already covered in part through the Regulation of Investigatory Powers Act and the pending Communications Data Bill.

¹² Enabled by Section 2(4) of the Identity Cards Act 2006.

¹³ 'Automatic voter listing 'could plug gaps in register'', Patrick Wintour, The Guardian, August 5, 2005.

¹⁴ 'Wider use of private data planned', BBC News Online, September 13, 2006.

- Disclosure of personal information held by local authorities to central government agencies and police;¹⁶
- Bulk disclosure of banking and communications administrative data to television licence enforcement authorities;
- Disclosure of spending habits and product transaction data to government for purposes of monitoring personal carbon usage;
- Routine disclosure of farmers' personal financial details to EU farm subsidy programmes;
- Disclosure of individual school and university academic and schooling records to funding authorities, and disclosure of personal financial details of families to access regulator to monitor university entrance;
- Data on students' course attendance and library borrowing passed to immigration and security services in bulk;
- Information from party conference registrations passed on from police to government departments and electoral commission;
- Census data passed to government departments.

Most of these scenarios are already in proposal form and some are mandated in existing legislation.

- If data are to be shared to a greater extent, the proposals create a substantially increased risk of security breaches of personal information;
- The data sharing provisions in the Bill were not put out to public consultation and are thus in violation of the spirit of the government's own code of practice on consultation;
- No Regulatory Impact Assessment has been conducted on the data sharing provisions in the Bill;
- In its current wording, the Bill contains Order-making powers related to data sharing that are not subject to independent oversight, and over which the Information Commissioner has no control;
- The involvement of the Information Commissioner as the co-leader of a crucial review into data sharing, together with his support for greater data

¹⁵ Passenger records (PNR) are already disclosed to US authorities. The EU is currently identifying the potential use of such transfers across European borders.

¹⁶ 'Fears of 'Orwellian dystopia' as councils, police and fire chiefs agree to share information', Jon Land, 24dash.com in Local Government, May 12, 2008; and 'Nowhere to hide for council tax dodgers', Observer, July 31, 2005.

sharing, has rendered his Office incapable of intervening in the proposed data sharing provisions;

- The acquiescence of the Information Commissioner to these proposed powers, albeit in a private capacity, gives every appearance of constituting a covert arrangement to provide greater funding and power to the Commissioner in return for his support for the clause 152 provisions.

Historical background

Since the late 1990's, at a time of the emergence of e-government initiatives, the UK government has focused much effort on the concept of "joined-up government" which would allow the seamless flow of information between departments. Later manifestations of this ambition were seen in strategies such as "modernising government" and "transformational government". By 2002 the ambit had widened to include data sharing between and within the private sector.

One of the key challenges in providing such a default real time flow of data across numerous areas of government and the private sector has been the issue of conflict with the provisions of the Data Protection Act, which provides that personal data collected for one purpose cannot be used for another purpose or shared with an unrelated entity without either an overriding public interest or the informed consent of the person to whom the data relates.

This provision is intended, for example, to prevent the default sharing of health data between the NHS and commercial medical researchers without patient consent or the arbitrary disclosure of police intelligence files to the insurance industry.

While there are a number of conditions that provide a mechanism for sharing of personal information (contracts, specific legislation etc), there is no way by which government can currently create a multiple layer sharing arrangement between agencies for a variety of specified and unspecified purposes. To do so would fundamentally breach core provisions of data protection law.

Despite this conflict, the government made a decision in 2007 to develop a long-term strategy to shift the general position of law from one of individual consent, to one of default sharing. In October of that year HM Treasury published the *Service Transformation Agreement*, an instrument near the core of the joined-up government agenda. The Agreement sets out a framework for action on changing public services to "more often meet the needs of people and businesses, rather than the needs of government". To achieve this ambition, a data sharing capability must be introduced. The Agreement states:

A.5 The MoJ is leading a cross-government programme to deliver a package of measures over the next 3-5 years to overcome current barriers to information sharing within the public sector.

In response, the campaign group NO2ID reasoned:

*We think that the “barriers” are not random obstacles. They are principles that have evolved in the courts and been captured in statute precisely because they protect things in human life that are worth protecting.*¹⁷

The document did not identify specific approaches to overcoming these barriers. However by the time of publication of the Agreement a decision had been made by government on a strategy to achieve this aim.

The Thomas-Walport Review on Data Sharing

Mindful of the need to deal head-on with the conflict with rights under the Data Protection Act, the Ministry of Justice later that month commissioned a review of data sharing provisions and limitations. The two people it chose to undertake this task were Dr Mark Walport, (now Sir Mark at January 2009) Director of the Wellcome Trust (a major user of health research data) and UK Information Commissioner Richard Thomas. Mr Thomas was a natural choice for the inquiry, given his knowledge of Data Protection law. He had also expressed concern about his limited powers and inadequate budget, and appeared anxious to raise the prominence of Data Protection. The review provided an ideal opportunity to press for these improvements.

The Terms of Reference for the review were:

Consider whether there should be any changes to the way the Data Protection Act 1998 operates in the UK and the options for implementing any such changes

Provide recommendations on the powers and sanctions available to the regulator and courts in the legislation governing data sharing and data protection

Provide recommendations on how data-sharing policy should be developed in a way that ensures proper transparency, scrutiny and accountability

Remarkably, Thomas agreed to conduct the review as an individual rather than in his capacity as Information Commissioner. This situation provoked disquiet, with some observers claiming conflict of interest. Indeed it is difficult to recall a similar situation arising with any other regulator. It can be reasonably argued that court judges are permitted to head up inquiries in their personal capacity, but not if the investigation conflicts with their jurisdiction or interests. However, a telecommunications regulator would encounter substantial criticism if a decision was made to lead, in a private capacity, an inquiry into competition issues in the telecommunications sector.

This decision had the effect of placing the Office of the Information Commissioner in an impossible situation in terms of commenting on the Review’s recommendations.

A two-month public consultation commencing in December 2007 followed the announcement of the Review. More than 200 individuals and organisations submitted comments.

The consultation was exceptional in two respects. First, the document was targeted specifically and openly at data protection specialists who were assumed to have knowledge of data sharing and the data protection legislation. Second, the paper

¹⁷ NO2ID Parliamentary Briefing on the Coroners and Justice Bill 22 January 2009

contained no substance or any discussion of scenarios or options, merely a questionnaire. At no point did the document indicate that its findings would feed into a legislative process. This format might be regarded as an inadequate consultation mechanism, in part because the general public was not involved in consideration of the issues that directly affect it, and second, because no factual base was established to anchor the responses.

Some of the Review's subsequent recommendations, published in July 2008 in the final report, were indeed controversial. Rather than focusing on reinforcing the primacy of the consent principle by suggesting measures to strengthen the Data Protection Act, the review recommended adopting procedures to streamline and entrench data sharing provisions:

Recommendation 8(a): *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.*

From the perspective of data protection, the final report was nothing short of scandalous, routinely adopting pragmatism in place of principled support for the core data protection right of consent. The legal position of consent was rarely addressed:

We support the instinctive view that wherever possible, people should give consent to the use or sharing of their personal information, allowing them to exercise maximum autonomy and personal responsibility.

This statement – like many others in the report – is remarkable in that support for consent should not be instinctive, but actual. It is embedded in law. That the report did not provide suggestions on how to strengthen that right, highlighted an agenda in favour of increased sharing of data. While raising some useful and important practical aspects relating to consent, the report concentrated on the challenges that this right posed to organizations and the need to circumvent consent:

It is unrealistic to expect individuals ever to be able to exercise full control over the access to, or the use of, information about them. This is because of a number of factors, not least practical difficulties in seeking and obtaining consent in many circumstances.

In other places the final report does acknowledge the importance of the data protection principles, though in each case it instituted a vast array of caveats and counter-examples of failure:

The problem does not seem to lie with the [Data Protection Act's] data protection principles. These are in themselves sound, balancing individual protection against the wider need to process and share information. They

provide a sensible approach to handling and processing data, neither inhibiting nor promoting data sharing. However, our consultation has indicated unequivocally that the Data Protection Act does not, and maybe by itself cannot, provide a sufficiently practical framework for making decisions about whether and how to share personal data.

In a similar vein, Privacy International does not call into question the legitimacy of the principles or their supremacy. As with the findings of the Data Sharing Review, we have concerns about the application and management of some of the rights. However, unlike the Review, we believe this should not imply that the wheel should be reinvented or that data protection rights accepted internationally requires debate or revision. If there is to be a debate on the principles, that discussion should be intended to result in the strengthening of those provisions, rather than their dilution.

Privacy specialists have rightly observed that is too often the case that arguments for “modernisation” of rights such as those at the core of the transformational government agenda are merely disguised attempts to destroy those rights. On the face of the evidence, this appears to be such a case.

Five days after the submission of the review’s final report the government announced a consultation on improved powers and increased funding for the Information Commissioner with a fast-track six-week submission phase. This is in stark contrast to the minimum twelve-week consultation period set out in the government’s Consultation Code¹⁸, possibly indicating that decisions had already been made on the matters contained in the consultation. Additional powers and funding were subsequently granted to the Commissioner.

Legislative overview

The provisions for the sharing of data between government agencies and commercial entities are contained within the Coroners and Justice Bill 2009, which is scheduled for second reading debate in the House of Commons on Monday 26th January 2009.

The provisions (all of which are contained in Part 8) do not constitute the main thrust of the Bill. Indeed the summary on the face of the Bill is somewhat misleading and could easily lead to an impression that amendments to the Data Protection Act to permit sharing are entirely centred on modernising coronial procedures. Part 8, however, provides for a general power and is not in any limited to matters of judicial process. Neither the concept nor the phrase *Data Sharing* appears in the Bill summary:

A Bill to amend the law relating to coroners and to certification and registration of deaths; to amend the criminal law; to make provision about criminal justice and about dealing with offenders; to make provision about the Commissioner for Victims and Witnesses; to make provision relating to the security of court and other buildings; to make provision about legal aid; to make provision for payments to be made by offenders in respect of benefits

¹⁸ ¹⁸ Department for Business, Enterprise and Regulatory Reform, Code of Practice on Consultation, July 2008, available at <http://www.berr.gov.uk/files/file47158.pdf>

derived from the exploitation of material pertaining to offences; to amend the Data Protection Act 1998; and for connected purposes.

Clause 152 of the Bill introduces a new Part into the *Data Protection Act* to allow for ‘information sharing’ of data if approved by an Order made by a Minister. These proposals seem to have come about because of a recommendation made in the *Data Sharing Review Report*. The government consulted on a number of the recommendations proposed in the report, but recommendation 8 which proposed this type of data sharing was not included as part of the consultation.¹⁹

In its Second Reading briefing on the Bill, Liberty observed that the clause 152 powers are:

...extraordinarily broad and make a mockery of the safeguards contained in the DPA. The amendments would enable the Secretary of State, Treasurer or a Minister in charge of any government department to make an order giving “any person” the right to share information, including personal data, by disclosing it to another person or using the information for a purpose not related to that which the information was initially obtained.

The power is not restricted to sharing between government departments. It could allow a private company to share personal data so long as an order was made allowing it. The examples given in the Explanatory Notes of the type of sharing involved include “when one company provides its client list to another company for commercial purposes” as well as where a government department obtains information for tax purposes but later uses that information for the provision of benefits and credits²⁰. The *Liberty* briefing rightly observes that the example could be turned around so that information obtained for benefits could be used to form the basis of a tax investigation. Equally, NHS data might be provided to health insurance companies or – as is being currently proposed – insurance company data might be transferred *en masse* to the DVLA.

The Bill stipulates that the only limit on the entitlement to make such an order is that the information sharing must relate to a matter with which the relevant Minister or department is concerned; it is to secure a policy objective that the Minister has; the provisions in the order are proportionate to the policy objective; and it strikes a fair balance between the public interest and the interests of any person affected by the order. Such an order can confer power on any person; remove or modify any legal prohibition on information sharing and amend or repeal any Act of Parliament whenever passed.²¹

The examples given in the Explanatory Notes state:

Before an order is made a general invitation must be given to all those who might be affected by the order to make representations and the Information Commissioner must be given a copy of the order and may submit a report in

¹⁹ Liberty (national Council for Civil Liberties; Second reading briefing. January 2009

²⁰ Paragraph 692 of the Explanatory Notes.

²¹ Liberty second reading briefing.

relation to it (which must be laid before Parliament), but he has no power to amend the order. The order must be approved by Parliament, but Parliament has no power to amend the order.

If these amendments are enacted it will give Ministers the power, through secondary legislation, to effectively nullify the protections contained within the DPA, and indeed the very purpose of the DPA.

In effect, these amendments would permit a Minister to allow any person (including a company or another government department) to share information about any person (including company information) as well as personal information that they hold on any person (e.g. name, address, date of birth, ethnicity, credit history, medical records, DNA and genetic information, tenancy records, social work records etc), if to do so serves the government's policy objectives.²²

The objective of channelling patient data to the medical research sector without patient consent has been made clear by government on numerous occasions. With regard to the data sharing proposals, the Rt Hon Dawn Primarolo MP, Minister of State for Public Health, told the House of Lords Science and Technology Committee:

Everyone in front of you and the Government is absolutely determined to exploit this research opportunity. In fact, Lord Drayson and I were discussing how unique it is in this country that we have this cradle to grave community into specialist care data and to link that to genomics is very powerful as a way of learning how to improve public health and individuals' care. That's why we are making substantial investment in this research capability programme for NHS Connecting for Health... ”²³

When former health minister Lord Warner stated that: “*the great prize for researchers in this area is being able to access the current data that is in the medical record plus the new genomic data as it emerges for individuals*”, the Minister replied “*I agree. If they are linked for clinical purposes then the only issue is about access and as long as we develop safe havens effectively to pseudo-anonymise...then we'll be all right*”. However, the minister refused to be drawn on whether Government would revisit legislation to make access easier, stating: “*At the moment it's two steps*”.²⁴

The view of the Information Commissioner

The commentary offered by the Office of the Information Commissioner makes for interesting reading. In contrast to the stark assessment presented by a range of legal experts who believe the DPA principles will be crippled by the provisions in the Bill, the Information Commissioner is adamant that the DPA protections will stand:

²² *ibid*

²³ ²³ Rt Hon Dawn Primarolo MP, Minister of State for Public Health, Rt Hon Lord Drayson, Minister of State for Science and Innovation, Universities and Skills, Professor Dame Sally Davies and Mr Mark Bale, Department of Health (2009) Oral evidence to the House of Lords Science and Technology Committee Inquiry on Genomic Medicine. 21st January 2009. Available for 28 days from 21st January on: www.parliamentlive.tv

²⁴ Genewatch; **The Coroners and Justice Bill: A DNA database by stealth?** Parliamentary Briefing, January 2009

Some have suggested that the Bill's information sharing provisions represent an unwarranted interference with the privacy of personal information. We do not agree. The provisions of the DPA will continue to apply to the sharing of personal information whether undertaken within the scope of an information order or otherwise.²⁵

And with regard to action that may be taken with respect to Orders:

The Bill rightly provides for ICO to produce a report to Parliament when a Ministerial information-sharing order is introduced – preferably after a privacy impact assessment has been undertaken. Our report will address the proportionality of the information sharing and its effect on individuals. It will allow us to ensure that safeguards are in place and that individuals' rights are respected.²⁶

This analysis misses one of the most important concerns. The core issue is not whether Data Protection Act protections will apply to data sharing affected by an Order, but whether some of the principles must be circumvented in order that the sharing can be performed in the first place (i.e. the core purpose of clause 152). That is, currently NHS data *cannot* be transferred *en masse* to private sector medical research organisations. Under the new provisions, such a transfer can take place as long as the remaining principles of the Act (security, access etc) are enabled. It is no stretch to liken this situation to one where health & safety protections are enforced for prisoners on *Death Row*.

There is nothing in the information sharing expressly stating that the sharing of personal data has to be consistent with the Commissioner's Code of Practice. The absence of this link allows information sharing to occur if a Minister decides it is necessary to secure a policy objective etc in circumstances where the sharing actually disregards the Commissioner's guidance if need be.

A Minister may, for example, 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 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).

The Commissioner also claims:

Where appropriate, we will be able to advise Parliament that a particular initiative is a step too far, or that further safeguards are required.

This assertion is misleading. There is no provision in the Bill to require Parliament to take action on advice from the Information Commissioner. Even if such advice was to be taken seriously, Parliament will be unable to amend an Order. In such a case the only influence that can be exerted by the Commissioner is to intervene before an Order is issued.

²⁵ Coroners and Justice Bill: A commentary from the Information Commissioner's Office – Second Reading 26 January 2009

²⁶ *ibid.*

There are significant concerns about the fairness of the parameters set out in the Bill for issuing an Order. As Liberty notes:

Further, the requirement to “strike a fair balance” between the public interest and the interests of an individual is a convenient yet misleading analysis that involves weighing up the greater good against a particular individual or group of individuals, who will often be hard pressed to show that their interest outweighs the greater public interest. It is only by aggregating the impact of the order across the many people who may be affected that the real extent of the privacy infringement can become clear.²⁷

Many of these problems arise because of the Order-making powers conferred to government, a trend that has now become conventional practice.

While authorities must submit a copy of a draft order to the Commissioner there is no obligation to disclose to the Commissioner any background document or legal advice about an Order, no obligation to answer any request for information from the Commissioner and no obligation to engage the public about the detail of a draft Order. In practice, according to the wording in the Bill, this means that representations can be ignored after they have been considered.

The *Joint Committee on Human Rights* has already heavily criticized this mechanism in respect of the appropriateness of leaving data protection safeguards to secondary legislation. In its fourteenth report the Committee observed:

We fundamentally disagree with the Government’s approach to data sharing legislation, which is to include very broad enabling provisions in primary legislation and to leave the data protection safeguards to be set out later in secondary legislation. Where there is a demonstrable need to legislate to permit data sharing between public sector bodies, or between public and private sector bodies, the Government’s intentions should be set out clearly in primary legislation. This would enable Parliament to scrutinise the Government’s proposals more effectively and, bearing in mind that secondary legislation cannot usually be amended, would increase the opportunity for Parliament to hold the executive to account²⁸.

Zero consultation

The government’s latest code of practice on consultation²⁹ fails to set out requirements for circumstances in which a formal consultation process is required. Such decisions, it advises, are the prerogative of government. Nevertheless the introduction to the Code advises:

When developing a new policy or considering a change to existing policies, processes or practices, it will often be desirable to carry out a formal, time-

²⁷ C.f. Liberty briefing.

²⁸ *Data Protection and Human Rights*, 14th report 2007/2008, 4 March 2008, paragraph 20 available at: <http://www.publications.parliament.uk/pa/jt200708/jtselect/jtrights/72/72.pdf>

²⁹ Department for Business, Enterprise and Regulatory Reform, Code of Practice on Consultation, July 2008.

bound, public, written consultation exercise. This kind of exercise should be open to anyone to respond but should be designed to seek views from those who would be affected by, or those who have a particular interest in, the new policy or change in policy.

While it is usual for a formal consultation to be invoked in the case of primary legislation, the Code offers the caveat: “there is no point in consulting when everything is already settled”. Given the history and circumstances of the data sharing proposals, this would seem to be the case.

For reasons set out earlier in this report, the *Data Sharing Review* cannot be viewed as a formal public consultation. Instead, it is a question-based document containing no substance or options.

While it is fair to say that the bulk of the *Coroners and Justice Bill* was subjected to reasonable public review and scrutiny, the Part 8 provisions were largely ignored. By its own admission, the Data Sharing Review was targeted at experts and specialists, rather than the stakeholder group most affected – the public. In contrast, the parts of the bill dealing with improvements to the coronial and inquest procedures were the subject of numerous publications and full consultations.³⁰

Summary

This policy has been the overarching vision of the UK Government since the late 1990s. We are surprised it has taken so long to devise a policy of this breadth and with such disregard for even the most basic safeguards. Despite continuous debates about genetic databases, health databases, and biometric databases, everything has been done to ignore debate on this policy. This can serve only to destabilise any decision made by Parliament on these other matters.

To conclude, the problems with this law are as follows:

1. Based on an illegitimate consultation process over a ten-year period, created to justify whatever the Government drafted into law. Even the Information Commissioner’s Office has been compromised.
2. Avoids Parliamentary scrutiny by pushing orders through secondary legislation.
3. Consists of meaningless protections and oversight, where the ICO may provide comments to Parliament in a process where Parliament is not permitted to amend the order.

³⁰ For a partial list see the legislation pages of the UK Parliament at <http://www.commonslider.gov.uk/output/page2655.asp>