

The British Computer Society's (BCS) Concerns about the Data sharing Implications of the Coroners and Justice Bill

1 Introduction

Buried in the government's Coroners and Justice Bill¹ are proposals to make very significant changes to the Data Protection Act (DPA)1998. The changes propose enabling any government minister(s), following the approval of the Secretary of State responsible for data protection matters, to make an Information Sharing Order enabling any designated person or organisation to share specified information which includes at least some personal data, providing it is **necessary to secure a relevant policy objective**. The definition of **sharing** is changed to include using the information for purposes other than those for which it was collected. Almost any information can be shared under an Order – a person or company's financial details, intelligence about them/it collected by the police, a person's DNA analysis, GP, clinic or hospital records, social service or criminal history. It also sets out the role of the Information Commissioner vis-à-vis Information Sharing Orders, including obliging him to produce a Data Sharing Code of Practice.

An Order may **amend, add to, revoke or repeal** any existing law, and can confer powers on the promoter, for example to require sharing or to override an existing obligation of confidence, and enables them to create new classes of offence carrying fines and/or imprisonment, for example for refusing to share when ordered to do so. An Order may remove or modify any existing limits on onward sharing of the information by the person seeking to share it.

These powers are very wide ranging and general.

2 What checks and balances does the Bill propose to constrain these powers?

At the very least, such powers require compensating checks and balances to prevent their abuse. However scrutiny of the Bill suggests that elements of it that on first sight seem to offer these protections do not in fact do so:

- 1 The Information Commissioner receives a copy of each proposed Information Sharing Order and may submit comments on it to the Secretary of State. However clauses 152-154 imply that the Commissioner may not comment on whether the Order is **necessary to secure a relevant policy objective**, and the Secretary of State is under no obligation to take account of the Commissioner's response.
- 2 Information Sharing Orders are only subject in Parliament to the very limited scrutiny offered by the affirmative resolution procedure before being voted on. The procedure permits very little time for debate, and what there is may take place in Committee if a government so wishes. Their effectiveness has been questioned by many, including established parliamentarians. This is no way to examine Orders that can create new offences punishable by imprisonment.
- 3 An Information Sharing Order may **amend, add to, revoke or repeal** any previous legislation, for example the Human Rights Act, that stands in its way

¹ See Coroners & Justice Bill, Part 8, clauses 152-4 and Schedule 18

- 4 The Bill does not say that an Information Sharing Order must conform to the current Data Sharing Code. The Code is not legally binding, and there is no penalty for breaking it. The Code only applies to personal data, while Information Sharing Orders can encompass more than personal data.
- 5 The Code is a code of practice, and deals with how information is shared, not the necessity of any sharing.
- 6 A Secretary of State seeking an Information Sharing Order has the power to reject the Code (designed to provide safeguards against abuse), and so can prevent it from being laid before Parliament until a version is submitted that is to his or her liking.
- 7 As it stands, the Bill effectively enables the Secretary of State to evade Data Processing Principles 1 – the fair processing requirement, and 2 – use only for the purpose stated, vide the Bill's redefinition of **sharing** described above.

3 Conclusions

We struggle to see the justification for these data sharing proposals. To claim, as the associated explanatory material does, that clauses 152-154 are needed to enable all agencies to be informed of someone's death is risible: there are much easier and cheaper ways of doing that. As a response to the Data Sharing Review, the proposals go much further than its recommendation for a fast track procedure to be used exceptionally by the Secretary of State in 'precisely defined circumstances', and runs counter to its advice 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'. We have heard a view that the Data Protection Act 1998 already permits the Secretary of State to achieve at least some of the major objectives of this Bill.²

BCS has made representations to Her Majesty's Government and its agencies on several related topics over the last year or so, including the [Data Sharing Review](#), the proposed [National Identity database](#), the NHS Connecting for Health questionnaire on the [additional uses of patient data](#), and most recently the House of Lords Select Committee on the Constitution, 'Surveillance: Citizens and the State'. The common theme of our responses, based on detailed consultation with members of the IT profession and others, is concern about the burgeoning power of the state vis-à-vis the citizen.

In 2008 BCS commissioned a [survey](#) of public attitudes on data guardianship, and produced a Personal Data Guardianship Code after wide consultation inside and outside BCS with positive results. Responses to the survey indicate that over three quarters of those questioned considered that data protection was important to them, and over 90% that they should be asked for consent before their data was used for purposes other than those originally intended. There is no requirement in these proposals to obtain the data subject's consent: in fact the proposals do not mention data subject consent at all.

The proposals conflict with the ethical codes practiced by several large professional groups, among which are clinicians and health informaticians³. This issue is at the

² Data can be made available under the Data Protection Act 1998, using Schedule 2 5(c) & (d) and 6(2) for personal data, and Schedule 3, 7 (1c) and 7 (2a) for sensitive personal data.

³ A handbook of Ethics for Health Informatics Professionals', A PDF form is available at <http://www.bcs.org/server.php?show=conWebDoc.1379>

heart of the BMA response to the proposals which says 'it appears to permit an unprecedented sharing of confidential personal health data... This Bill strips patients and doctors of any rights in relation to the control of sensitive health information'. We agree with this statement.

BCS believes strongly that the process being used to introduce Information Sharing Orders as part of a much larger bill concerned with other matters precludes sufficient public debate, discussion and parliamentary scrutiny of proposals that involve novel and very general – some would say draconian - powers of great significance to every UK citizen and organisation. Introducing the proposals as a bill in its own right would remedy this.

We also believe that the proposals will be open to challenge under Article 8 of the Human Rights Act, and other related EU and international obligations of the UK. BCS believes that, if implemented, the Bill would:

- traduce the original intention of the DPA 1998, notably its first two – and arguably most important – principles, and the primacy of subject consent. The redefinition of **sharing** to include the use of data for purposes other than originally stated will cause public and legal confusion, and should be dealt with separately.
- severely weaken the independence of the Information Commissioner. Although the Commissioner is obliged to produce a Data Sharing Code and subsequent versions of it, they require the approval of the Secretary of State and are not subject to thorough Parliamentary scrutiny. The Bill provides no sanction if a person does not comply with an assessment notice issued by the Commissioner, but does provide a formal right of appeal against such a notice. The proposals would effectively concentrate control of people and organisations' right to data privacy entirely in the hands of the Secretary of State. We therefore support the submission of the Information Commissioner to the Bills Committee. However we believe the Bill will have a more deleterious effect upon his independence than he suggests.
- heighten the distrust citizens have of government and central initiatives, and thereby set back the efforts of government and its agencies to provide faster, more cost-effective public services using IT.
- damage – possibly wreck – the existing efforts of those currently trying to openly persuade citizens to accept that large scale storage, use and appropriate sharing of personal – sometimes sensitive – information will not prejudice their data privacy. A prime example is the development of a National Care Records Service for NHS patients.

Of the forty or so inputs we have received directly on these proposals from people inside and outside BCS, all agree on one thing: these proposals are far too ill-defined and general for their stated purpose, are as a result potentially dangerous, and will do more harm than good. As experience in the last century and elsewhere suggests, it is unwise to rely on the benevolence of a government to sensitively deploy such wide-reaching and general powers as these. In the wrong hands, it would permit the restriction - and ultimately the destruction - of the right to personal and corporate data privacy.

Ian Ryder
Deputy CEO, The British Computer Society
Tel: +44 (0)1793 417751

16 February 2009