

## Personal Identity Working Group

Drafted by: Dave Wright  
Date prepared: 18/01/05  
Date finalised: 24/01/05

Circulation: PI Group

THE EUROPEAN  
INFORMATION  
SOCIETY GROUP

EURIM



### Summary report of the EURIM Personal Identity Group meeting held on 13 January 2005, 1330-1730, Room S, Westminster Palace

Chair: Paul McKeown (IBM)  
Rapporteur: Dave Wright (EURIM)

#### **1. Introduction**

1. The purpose of the meeting was to present short talks on selected data-sharing models, with the aim of integrating existing and proposed consent-driven models, and to use this to construct the first draft of a EURIM model of data sharing, in association with DCA if possible.

#### **2. Data sharing: a summary of guidance from the Department of Constitutional Affairs**

2.1 A summary was given in layman's terms of the information available on the DCA website about the law on data sharing. The summary below should be read alongside the document 'Presentation - DCA talk' which is on the EURIM website at <http://www.eurim.org.uk/activities/pi/pi.php>. More details can be found at: <http://www.dca.gov.uk/foi/sharing/toolkit/lawguide.pdf>.

2.2 There are 4 main elements in the DCA document on data sharing:

- Administrative law;
- The Human Rights Act 1998 and the European Convention on Human Rights;
- Common Law, statutory obligations of confidence and statutory restrictions on the disclosure of data;
- Key elements of the Data Protection Act 1998 relevant to data sharing.

2.3 Administrative law refers to the carefully defined powers (*vires*) of public bodies with regard to sharing information. Departments can be of two types: those that are headed by a Crown Minister such as the Treasury, the Home Office, the Department for Work and Pensions, the Department for Education and Skills etc., and those that are created by statute and that are not headed by a Minister, such as the Inland Revenue and Her Majesty's Customs and Excise.

2.4 One might suppose that unless the right to share data is defined in a particular statute, it would be banned, but this is not the case because ministerial departments derive their powers to collect, use and share data from express statutory powers, implied statutory powers and prerogative or common law powers. Government departments that are established by statute do not have prerogative or common law powers, but must look to their statutory powers (express and implied) to provide a legal basis for data collection, use and sharing.

2.5 The Human Rights Act 1998 (HRA) came into force on 2 October 2000 and it gives effect to the principal rights guaranteed by the European Convention on Human Rights. The Convention was adopted by the Council of Europe in 1950 and ratified by the United Kingdom in 1951. Articles 8.1 and 8.2 are relevant:

- 8.1 Everyone has the right to respect for his private and family life, his home and his correspondence.
- 8.2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the

prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 8 is a qualified right that allows a public authority to interfere where that interference is:

- in accordance with law;
- in the pursuit of a legitimate aim; and
- necessary in a democratic society.

Briefly, the first element requires a legal basis to permit data sharing: legislation, delegated legislation, the common law and even rules of a professional body may suffice. The second element means that the data sharing must be for one of the purposes specified in Article 8.2. It is usually fairly easy to satisfy this requirement. Satisfaction of the third element will probably be the key factor in the majority of cases; courts are required to look at all the circumstances of the case and assess whether the exercise of the power was 'proportionate' – case law is often relevant here.

2.6 The law of tort is an area of civil law that provides individuals with a cause of action for damages if there is a breach of legal duty. As regards the collection, use and disclosure of personal information, the tort of breach of confidence is of particular relevance. Breach of confidence is a tort, which protects information under certain circumstances.

2.7 Government departments and local authorities that have access to confidential information relating to citizens may owe duties of confidence. In relation to information held by public authorities the same principles apply as would apply to information held by private persons and organisations. For the purposes of the law of confidence it is clear that different government departments are treated as separate legal persons which means that information cannot be freely disclosed between government departments without taking into account the common law of breach of confidence.

2.8 Other legislation provides for a power to make disclosures in certain circumstances, e.g. s115 of the Crime and Disorder Act 1998, which gives the power (but not the requirement) to disclose information where necessary: the case for disclosure would need to be balanced against any competing obligations (such as confidence).

2.9 Related to civil obligations of confidence are statutory obligations that may prohibit the disclosure of certain types of information by imposing specific obligations of confidence (e.g. information supplied to the Child Support Agency).

2.10 JH summarized details of the eight principles for data protection as they affect data sharing, and concluded that a public sector body can share data for any reasonable purpose if it wants to.

### **3. Data Sharing: different models and approaches**

3.1 Presentations were given by other members present and are on the EURIM website at <http://www.eurim.org.uk/activities/pi/pi.php>. They can be loosely described as the 'Eidentity', 'IBM', 'Fujitsu', 'Microsoft' and 'Experian' models. The presentations form the basis for the discussion below.

### **4. Discussion**

4.1 Discussion of the presentations focussed on the possibility of integration of the various models. A key consideration was compatibility: are the models sufficiently similar that they can be integrated to advantage, or do we need to choose between the 'Virtual Home' (Eidentity) and 'Experian' models?

4.2 We could pull out the themes within the various models, evaluate them for compatibility and look at the technology behind them. The VH model is citizen-centric, whereas the Experian model is organisation-centric but works with or without consent; the 'IBM' model and others would appear to be in between. However, it is clear that they do share significant commonality, including a requirement for secure identity management and authentication, the requirement for a trusted intermediary or equivalent, and the need to identify or remove legal and cultural constraints.

4.3 Concern was expressed about 'generic' solutions, because it is likely that different situations will require different solutions. Would a data-sharing process work if not computer-based? Are there commercial or political priorities that we should consider in choosing which model to adopt? A clear recommendation from the subgroup should be that the adoption of any data sharing model should be

proven in an internal pilot scheme before being applied more widely. A second recommendation should be the requirement for an assessment of the impact of not sharing data.

4.4 It is clear that the transformation of service delivery is a key Government priority under the Gershon efficiency agenda. A pilot scheme might involve a trusted intermediary acting on behalf of the individual and acting as his/her agent; this would generate trust and offer clear value and benefits for both the individual and Government. This could be applied by linking existing infrastructures through common standards and shared databases, but the pilot would have to be chosen with care. Any scheme would be paid for by the data requestor.

4.5 A possible limitation on the VH model might be the inability or unwillingness of individuals to actively manage their identity. Where the system controls procedures, the most vulnerable in society are often those most often in need of Government services, but are the least capable of handling their own affairs responsibly. This needs to be borne in mind when choosing a data sharing model. The Government will want data sharing to work and generate efficiencies, and it will not want to depend on the individual to bring this about. Data sharing will be an important driver in service delivery.

4.6 It would be advantageous if the trusted intermediary was seen as an agent of the individual. However, the benefits of data sharing most attractive to Government are most likely to be manifested in anti-fraud success, cost savings linked to improved service delivery and release of resources to the front office. Perhaps we should therefore focus on developing a single model for presentation to Ian Watmore, based on the circle of trust model based on the consent-driven relationship between 3 key parties – the individual, the service provider and the trusted intermediary. This was compatible with most of the other models, although trust in one model was based on PKI rather than on other forms of identity authentication and eligibility. Using a trusted intermediary would also facilitate trust and simplify information management (and therefore reduce costs) for the Government department, e.g. by handling specific consent. In the VH model, every individual has an electronic relationship with every third party, while the intermediary facilitates authentication of the relationship effectively by having the third party pay for the authentication service.

4.7 Discussion continued to facilitate mutual comprehension of the detailed functioning of different models. This concluded by asking whether or not the models presented could be integrated, and if not, did this matter? Different models might be suited to different environments, according to the specific needs of the individual and the Government department. This should not hold back the group – rather, it provides flexibility. The VH model might lend itself more easily to the education field, whereas the circle of trust model might be more appropriate in the employment field.

4.8 The remit of the subgroup includes making a case to Ian Watmore for data sharing. A second aim is the production of a paper that points out the consequences of a failure to share data. The subgroup will continue to develop its thoughts on these issues before presenting its findings and recommendations to the full group.

## **5. Date of next meeting**

5.1 The date of meeting will be 20 January, Room S, Portcullis House, Westminster, 1330-1730.