



**Summary Report of the EURIM Personal Identity Subgroup meeting, 25 May 2005,
1400 – 1600 at Abingdon House, Westminster**

Chairman: Paul Mckeown (IBM)
Rapporteur: Dave Wright (EURIM)

SUMMARY OF MAIN POINTS

1. The data-sharing paper for Parliamentarians has been remodelled from the paper sent to eGU, and will focus on barriers to data sharing, but without the planned detailed appendix. The material should be assembled for Ian Stewart MP to review, before the end of June 2005.
2. A significant feature of the public sector is the 'toxicity' of relationships between departments and agencies, which works against any form of linkage. Would-be users of Government Gateway are inhibited from signing up by doubts as to whether Government supports its growth, with additional functionality, or plans to supercede it, e.g. by the NIR. This needs open debate.
3. There is no sign at present of a coherent, overarching strategy for managing personal identity and there are conflicting pressures arising from reports into damage/suffering/death caused by failure to share information and cases that have exposed unauthorised access to supposedly secure files leading to similar problems.
4. The current eGU objective is to have a National Strategy for Government IT ready for public announcement in November. Input to Government from EURIM on the development of processes for personal identity management and secure data sharing might be very useful in this context: the CIO Council will want solid proposals to emerge from its meeting in July.
5. The more detailed paper for eGU on identity relationships may be of use to those involved in developing an overarching personal identity strategy. **A straw man is being drafted for circulation to the group, with the aim of having material ready for the end of July, when the CIO Council is due to agree their core proposals.**
6. A major contribution the PI Group could make would be to stress the importance of data sharing protocols with respect to IT standards and processes, in addition to governance processes, data management etc. Any paper we produce would have to address the management and people processes, not just the technology. **Our aim should be to ensure that the CIO Council has political backing to deliver what is needed for successful implementation.**
7. **The material should therefore point towards least-risk routes for the implementation of data sharing and help raise political pressure in support of such strategies.** Champions, with budgetary authority to enable successful implementation across boundaries, are needed to drive forward programs in specific application areas.

1. Introduction

1.1 The purpose of the meeting was to progress the gathering of information for the educational brief on data sharing for Parliamentarians, and to assess the format and content of a draft paper on data sharing for eGU.

2. Progress on papers

2.1 The meeting was intended as a working session on the data-sharing paper for Parliamentarians being drawn up by the subgroup, a rough draft of which had been circulated yesterday. This had been remodelled from the paper sent to eGU, and was intended for a 'lay' audience rather than a technical one. The aim is to have material ready for use in briefing the new intake of MPs before the end of June 2005.

2.2 Progress so far included the current **tabled draft paper for Parliamentarians** - intended as a non-technical remodelling of the original paper sent to eGU, based on an agreed template. The bulk of the paper is expected to focus on barriers to data sharing. The material should be assembled for Ian Stewart MP to review, before the end of June, for consumption by MPs.

2.3 It was suggested that we abandon the proposed detailed appendix for the paper for Parliamentarians in the light of outcomes from the meeting with eGU, partly because of time constraints and partly because of the difficulty in defining models – the same words were being used in different ways in different definitions, and attempts at classification were proving problematical. The appendix will be replaced by a glossary (see S 2.13).

2.4 Some members felt that 2 distinct approaches to personal identity data management (centrally controlled and "federated") should be compared and contrasted. Others considered the main distinction to be that between compulsion and choice, but even this might be illusory. However, the physical location of databases is irrelevant - the issue is who controls access to the databases. Centrally-controlled databases can comprise multiple locations around the globe, but with access controlled through one index. Databases could then be accessed for data-mining purposes through non-duplicatable indices, should the controllers (public or private sector) decide data sharing was required.

2.5 The Government model is said to be for a central index to everyone in the country, and other Government databases can be linked to the index through the unique identifier. In a federated model, the Government would supposedly have no knowledge of how multiple identities linked across the different databases without permission from the individual. The federated solution is for the individual to have a token with different identities for the same individual (for the NHS, DVLA etc.), so that he/she can decide when a link can be established so that the departments/agencies can share data.

2.6 It may, however, be that neither model, as described, relates to the processes that Government is trying to put in place, which involve multiple identities on different databases (e.g. for 'every child matters'). Current proposals appear to be for a national biometrically-de-duplicated database (the NIR) with a very limited set of information and no intention to hold more than a few reference numbers. Access to health and tax records would supposedly not be possible through the national identifier number, though the ID system is intended to provide better proof of identity.

2.7 At the Government IT Summit meeting (25 – 26 May), panellists with experience of both public and private sectors discussed the differences between them. One of the most significant was the 'toxicity' of relationships between departments and agencies, commonly with different recruitment and staff development structures and cultures, no means of co-operation and little or no trust in each other's systems or people. This works against any form of linkage, whether centrally-controlled or federated, although federation, with single sign-on and access across a limited number of departments and applications, already exists in the form of Government Gateway. Would-be users are inhibited from signing up to the Gateway by doubts as to whether Government supports its growth, with additional functionality, or plans to supercede it, e.g. by the NIR. This needs open debate.

2.8 Categorising the approaches into central or federated appears to be an oversimplification of the models used in practice. The problem is one of terminology, in that different people attach different meanings to the same words; the real difference is between having a single identifier for all purposes, or having multiple identifiers, with the individual deciding which identifiers will be released to which

databases for which purposes. Central or personal control over how the databases are linked is the key issue.

2.9 Such simple choices are, however, unlikely in practice; elements of individuals' interactions with Government involve both central and personal control. Some departments have the ambition to link for some purposes to the NIR, but not necessarily for others. The extent to which this should take place needs explicit debate, to determine the approaches to the overall management of personal identity across government that are appropriate. Different applications may well require different approaches. If so, how can or should these be linked (e.g. ID card system, Government Gateway)?

2.10 There is no sign at present of a coherent, overarching strategy for managing personal identity and there are conflicting pressures. These arise on the one hand from the failure to share information (e.g. the Bichard Inquiry recommendations), and on the other hand, vulnerabilities related to a number of scandals exposing unauthorised access to database information (with derisory penalties imposed on the offenders as with Operation Glade). The political motivation is to find a coherent way forward from this conflict and the related issues of lack of trust and cooperation between departments. Moreover Sir Nicolas Montagu (former Chairman Inland Revenue) has suggested that savings from a single account for the individual (bringing together taxes and benefits) could be far greater than those envisaged in the Gershon or James reviews. **At the Govt UK IT summit on 26th May Ian Watmore said that the current eGU objective was to have a National Strategy for Government IT (as a whole) ready for public announcement at the UK EU Presidency event in Manchester (November).** The development of processes for the management of personal identity and secure data sharing should be integral to any such strategy.

2.11 **Input to Government from EURIM might be very useful in this context:** the CIO Council will want solid proposals to emerge from its meeting in July.

2.12 Local authorities are delivering front-line services to the citizen, and use identity to link to IT, but are not dependent on a single central database. Efficiency and delivery benefits arising from data sharing are likely to figure large in Government considerations.

2.13 A glossary might afford the most useful outcome for defining what is meant by the various terms used (e.g. 'federated' etc). This could be added to the original paper for eGU, which predicted that as the Subgroup's understanding evolved, its use of terms and their definitions was likely to change. **The updated terminology can be employed in the material we are assembling for the paper for Parliamentarians;** however, it was agreed that we should not proceed with the detailed appendices for House of Commons Library in support of the original paper to eGU. **JH agreed to draw up a draft glossary for circulation and comment.**

2.14 It was agreed that the term 'financial services' model be replaced because the consent-driven routines are used well beyond financial services (e.g. for vetting job applicants). The model has the advantage that individuals can have multiple identities (with optional linking) and there is provision for them to be notified when requests are made to the database. Government appears to have no plans to use this model itself but a growing number of departments/agencies are contacting those who use this model for assistance with checking references, preventing fraud and/or cleaning files.

2.15 Departmental autonomy is a major obstacle to any national strategy. The processes for cross-departmental interactions with citizens need to be well defined, because the applications can have very different requirements, including levels and degrees of process-dependent security, checking and sharing. There is also a need to distinguish between processes and databases. With different types of file, identity and process, the data-sharing strategy must, like Internet protocols, allow particular types of communication and linkages between very differently structured operations operating to different standards – including management and governance not just technology.

2.16 The more detailed paper for eGU on identity relationships may be of use to those involved in developing an overarching personal identity strategy. **JH said that he had written on this subject already, and would be happy to draft a straw man for circulation to the group. It was planned to have material ready for the end of July, when the CIO Council is due to agree their core proposals.**

2.17 Issues of residential churn and registration should be included in the paper, one reason being the significant proportion of individuals who access government services who may have multiple

residences or move regularly (e.g. students, trainees on rotation or contract workers) or have no fixed address (e.g. travellers or the homeless). There may be a need to allow for simple casework references, akin to those used by Barnados, whose programmes serve ~350,000 individuals, some with very good reason not to trust the authority from whose care they have fled. Sensitive data may also need to be excluded from computer systems because the cost of security is disproportionate to any putative value. One participant in EURIM's E-Crime exercise gained access during a security audit to a public sector "at risk" register using only tools and information obtained by Google searches.

2.18 One aim of the Citizen Information Project is to have a contact address for each person. The population register will be built on the back of the NIR, and sharing contact address information will save time. However, until that stage is reached, the ability of the State to access and share contact address information will be limited, because there is no mechanism for doing so. There can, however, be a very good reason for having contact address information, e.g. health screening programmes, which provide a strong benefit for both individuals and the general population.

2.19 Advice to Government should include consideration of the implications of data sharing for a range of issues, policies and regulations - the use of permissioning for linkages is relevant here. Different approaches to data sharing can be used, e.g.: back-office, without permission, and front-office, where individuals can present a "certificate" and give consent for their electronic records to be connected. Examples of how current methods operate in practice are needed to enable more informed debate.

2.20 Any overall strategy needs consider the current reality of around 1350 autonomous central government departments and agencies, plus those of local authorities and 'the third sector'. That implies an approach akin to the processes which created the 'TCP/IP' standards for information sharing which enabled the evolution of the Internet. But in addition to IT standards, we also need protocols for delivering and agreeing access requests to assure identity verification and authorisations, for the secure transfer of information (of known accuracy and reliability) in usable format and for recording the process for governance purposes. **It was agreed that protocols are needed for transferring data from one personal identity and information 'network' to another, and for linking those who wish to be linked: any paper we produce would have to address the management and people processes, not just the technology.**

2.21 The programme for developing the necessary protocols and acceptance processes will require complex issues to be addressed with co-operation between departments that do not trust each other. Such actions will build trust and rationalisation over time, or alternatively lead to the development of models that allow transactions between those that do not trust each other, as in the Identrus model. This comprises multiple layers and circles of trust to fit the semi-incompatible financial services regulations of most nations (including some where neither the banks nor the government are trusted).

2.22 Permissioning protocols need specific attention: how permission is elicited from government or from the individual, and how it is checked. Notification to the individual of access requests to their database, as in the Experian model, would be one way of addressing this and could form the basis for a recommendation. How citizens could control access to their data is another aspect. However, law enforcement investigations might well override normal permission processes, and should be reported to an oversight body.

2.23 It is planned to look in detail at permissioning protocols in an approach to Hounslow Council that involves data sharing and exceptions to the EURIM-DCA Data Sharing Process Map. In particular the exercise will examine the practicality of data sharing using the Process Map in different circumstances, e.g. where a section of a department shares with another section in the same department, or where sharing is external. Results might be incorporated into the paper for eGU if this could be done by July.

2.24 A major contribution the PI Group could make would be to stress the importance of data sharing protocols with respect to IT standards and processes, in addition to governance processes, data management etc. To avoid this mushrooming into a huge exercise, the paper should identify only as headings the different issues to be addressed. Discussion should be limited to the functions of the protocols, not the detail. **Our aim should be to try to ensure that the CIO Council has the political backing to deliver what is needed to ensure successful implementation. CS agreed to supply a number of headings.** It was agreed that JH would produce a 'straw man' as quickly as possible, and DW would circulate this and integrate any feedback so that all Subgroup participants were working on the same master draft.

2.25 The current outline of the draft paper for Parliamentarians reflects the balance of the debate within the Subgroup, and goes into too much detail with respect to the differences between models. **The outline should be developed, with more content on 'barriers to data sharing' and a focus on overall benefits sharing, because the benefits of data sharing may not be commensurate with the immediate costs as seen in departmental budgets. This presents a fundamental barrier to data sharing and to efficiency in Government that needs to be addressed either by a central delivery team with an overview of the benefits that can be delivered, or by permitting local budget transfer at the operational level. The apparently insuperable barriers to this are one of the main differences between public and private sectors.**

2.26 The assembled material is likely to be in demand when data sharing becomes a live political issue: both Treasury and Cabinet Office wish to move the Gershon agenda forwards, but there are a number of obstacles and minefields in the way. **The material should therefore point towards least-risk routes for the implementation of data sharing and help raise political pressure in support of such strategies.** Champions, with budgetary authority to enable successful implementation across boundaries, will also be needed to drive forward programs in specific application areas

2.27 Responsibility for overall policy with regard to the Management of Personal Identity and Data Sharing appears to lie with the DCA (Permanent Secretary, Alex Allan, first E-Envoy) but DCA does not have authority over any of the main application areas. Senior responsible owners are needed to drive these. The CIO Council appears well placed to secure agreement to the necessary professional standards, by ministers, in advance of the announcements in November 2005. Departmental funding might then be linked to performance and implementation targets for the 2006 spending review.

2.28 **The Personal Identity Group has observers from most of the major identity initiatives across central government and it was suggested that the Subgroup liaise with these, perhaps beginning with one of the most difficult areas, that of child protection.**

2.29 PM agreed to continue to work on the draft paper for Parliamentarians, **in particular on the barriers to data sharing.**

3. Date of next meeting and future actions

3.1 The date of the next meeting will be decided in the light of progress on the draft papers.

3.2 The most urgent current activity is to agree inputs to the new Government IT Strategy by the end of June. The CIO Council is due to agree their core proposals in July for agreement across government by November.