

Personal Identity Working Group

Drafted by: Dave Wright
Date prepared: 06/12/04
Date finalised: 10/12/04

Circulation: Group Members

THE EUROPEAN
INFORMATION
SOCIETY GROUP

EURIM



Summary report of the Personal Identity Subgroup meeting on Data Sharing, held in Room W3, Westminster Hall, 1000 – 1200 hours, Thursday 2 December 2004

Chair: Stephen Darvill (LogicaCMG)
Rapporteur: Dave Wright (EURIM)

SUMMARY OF MAIN POINTS

1. The purpose of the meeting was to clarify the perceived problems around public sector data sharing, and to plan forward actions.
2. A major objective of the group is to put the issue of data sharing into the context of how to improve service delivery to the citizen, and to identify whether barriers to doing this are legal, cultural or organizational. For example, is the barrier to combining human resource systems across some departments legal, or because there is no specific power to do so?
3. There appears to be a lack of will by public sector workers to share data, either because of inertia or genuine worries about the Data Protection Act (as opposed to hiding behind it). DCA had issued guidance for local authorities and others on when data sharing is permitted, but definitive answers to questions were not provided. However, DCA has shown interest in the EURIM Process Map, with a view to a collaborative approach.
4. A major issue is the reluctance of the public sector to share data with consent; all other forms of data sharing appear possible, either with or without a specific statute. The solution depends in large part on the definition of an organization, and where the boundaries lie between the various sectors.
5. One way forward might be the use of data verification in data sharing – the need to check the data held against other information in other Government departments. It does not seem unreasonable to have overarching legislation that allows any department to verify personal data in an application for a service by a citizen, by checking against another Government department's database without the need for that citizen's consent.
6. The subgroup identified 5 different types of data sharing:
 - verification - checking offered information against a database – is it correct or not?
 - acquisition – the service provider asks the data controller for access, ±consent
 - distribution – data controller's relationship with partners
 - common database – e.g. local authorities with integrated or shared database
 - data mining – e.g. which pensioners are claiming which benefits?
7. The subgroup proposes a paper linking failure to share data with the consequent loss of benefits to the individual and of savings to Government. In a consent-based system, an intermediary would effectively hold consent on behalf of the individual. The Head of the e-GU Ian Watmore has advocated the use of trusted intermediaries as a means of transforming service delivery in the public sector, and so this route offered real possibilities for the subgroup.
8. The subgroup will attempt to construct a model of data sharing based on the integration of 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. This model would be refined in subsequent workshops and a prototype presented to Ian Watmore.

1. Introduction

1.1 The purpose of this meeting was to clarify the perceived problems around public sector data sharing, and to plan forward actions.

2. Work to date

2.1 Much of the current work emanated from the EURIM Status Report published in July, and a major objective is to look at practical applications of the 'Circle of Trust' model. For example, the model might be applied to the University-Employer relationship, and this is actively being pursued. A parallel risk-assessment exercise is also being undertaken, intended to encourage Government departments to adopt this approach, rather than to pursue this within EURIM.

2.2 At a Local Government Association data-sharing conference on 17 November, the Minister for Constitutional Affairs, Baroness Ashton, invited feedback on a range of issues. Clear frustration in the audience was expressed at the emphasis given to legislative and regulatory exceptions to data sharing under the Child Act, as opposed to the reluctance to address the many problems facing practitioners. A panel including representatives from EURIM, DCA and SOCITM, focused on trust between the parties and the benefits to the individuals within the Circle of Trust model, data quality, information governance and legislative issues.

2.3 EURIM members are developing a process map to guide practitioners on data protection and sharing issues. The intention is to allow the data controller through a structured process e.g. when asked by a third party for access to their data. DCA seem to be very interested in this, and a meeting will be held on 15 December to discuss the process map in more detail. The Information Commissioner's office is reviewing the first draft, and members have updated the process map in the light of external legal advice. Information on exceptions is being acquired on various sectors, and will be integrated into the process flows.

3. Issues to be covered

3.1 Colleagues have spoken to client staff in the Home Office, DCA, Revenue and Customs etc., in order to put the issue of data sharing into the context of how to improve service delivery to the citizen. One benefit would be for sole traders and SMEs to be able to combine personal and business taxation, and though there appear to be barriers, these might be cultural and organisational.

There are legitimate questions of privacy and informed or implied consent, e.g. if an individual fills in a tax return, what are the implications of ticking a box enabling Inland Revenue to access VAT and other personal records. When submitting an application for credit, is consent implied for the bank to carry out background checks by looking at information held by financial service providers? What are the obstacles that stop this being done in Government, where there is a logical case for better service delivery? Why cannot the Pension Service share information with the CSA? What is needed to enable them to do so? Do we need new legislation, or clarification of existing law? We need to look at this.

3.2 A recent incident involved a low-earner who declared his income to the Inland Revenue and as a result, some 4 weeks later received a letter from the NHS informing that they were exempt from prescription and other NHS charges. Obviously, some data sharing is taking place!

3.3 There is a need for sharing information between silos within particular organisations and agencies, in order to improve service delivery and efficiency (driven by the Gershon agenda), but this may be countered by a negative mind-set within departments and agencies. For example, colleagues reported a perceived barrier to combining human resource systems across DTI, because there was no specific power to do so. So what would need to be done to enable a common HR system? Yet in some organisations, e.g. MoD, there are common HR services.

3.4 In Japan, changes to the law had been made to allow Government bodies and prefectures to work together, and to decide at what level common services would be best delivered. Some of the larger municipalities are operating through a common IT infrastructure to host their services, and early reports suggest that the system is delivering efficiencies

3.5 There are examples of successful data sharing projects in the UK public sector, but serious problems remain. Would a review of the DCA guidance identify what legal constraints existed to prevent data sharing? It was agreed to have a presentation on DCA had guidance for local authorities

and others on when data sharing is permitted, although definitive answers to questions are not provided. DCA have shown interest in the EURIM Process Map, and meetings are taking place with a view to a collaborative approach.

3.6 Data sharing can improve service delivery, e.g. where there are overlaps across organisational boundaries, e.g. for Council Tax billing, so why cannot a collection agency be set up for all London boroughs? What is the showstopper here? Organisational inertia? Privacy considerations demand that some vertical divisions within and between local authorities are required by statute, e.g. housing and social services, but a way could surely be found to share non-contentious data such as change of address information across the organisation.

3.7 Much depends on the definition of an organisation, and where the boundaries lie between the various sectors; local authorities may be construed as a number of different organisations operating under the same umbrella. Different LA's have different attitudes and practices – some departments share, others do not. So is it a question of practice, advice or legality?

3.8 How does the DPA defines an organisation? If a local authority arbitrarily decides to have a number of registrations, is that a choice they can make, or does the DPA specify at what level a service should be provided? At the other extreme, if there is just one entry for an organisation under the DPA, at which point is legislation needed to share information? What does European legislation say about how citizens exercise rights of access across multiple registrations? What is the logic behind how to define an entity, and what is the appropriate level of registration? At what level do data sharing problems arise, and at what level can they take place?

3.9 There are a number of initiatives that introduce a unique number for services; there is a unique number for every entity we deal with. The public sector resembles a federation of distinct entities at departmental or even service level. To what extent are unique numbers required in an IT world in which federation is becoming a sensible idea for sharing identities between distinct entities? A meeting attended by William Perrin (Policy Advisor, Prime Minister's Office) and Andrew Stott (Deputy CIO and Head of Service Transformation, E-Government Unit) to discuss to what extent unique numbers are needed in different sectors of the economy concluded that there appeared to be no legal answer.

3.10 Is there an issue of departmental control of the service it provided? Is the plethora of unique numbers a symptom of the malaise about data sharing? There are differences between departments – DoH has a command and control, top-down structure that has long used a unique number, whereas the DfES and LA's had a more federated, consensual approach. The lack of a cross-departmental strategy may also promote the use of numbers – departments tend not to talk to each other, and have no common goal.

3.11 Data sharing also depends on the purpose behind card issuance. If a card is used as an anti-crime measure, it would be important not to link it with other databases which might corrupt the information. If the intention is to facilitate citizen-Government transactions, then data-sharing links would be expected. Achieving the privacy-benefits link is the dilemma and challenge.

3.12 **The crucial question is: what is preventing Government from sharing what it wants to? Once this is established, we can move to the consent issue.** Consent would not make an illegal act legal; on the other hand, the advice offered to local authorities at the LGA conference on 17 November appeared to suggest that if there was a need, data should be shared!

3.13 Verification is an important element in data sharing – the need to check the data held against other information in other Government departments. It should not be unreasonable to have overarching legislation that allows any department to verify personal data in an application for a service by a citizen, by checking against another Government department without the need for that citizen's consent. For example, a verification check that a name and driving licence number are corresponding data should be legally possible. The ID cards legislation specifically enables the Secretary of State to verify the information used.

3.14 Verification checks at the point of entry into a system offer a simple way of cutting through many of the barriers to data sharing, although increasing degrees of data sharing and data integration might involve data mining and require more specific legislation. Anti-fraud and prevention of crime legislation

already allows data mining across Government; the grey area causing all the problems lies between this and social services.

3.15 Five different types of data sharing can be identified:

- verification - checking offered information against a database – is it correct or not?
- acquisition – the service provider asks the data controller for access, ±consent
- distribution – data controller's relationship with partners
- common database – e.g. local authorities with integrated or shared database
- data mining – e.g. which pensioners are claiming which benefits?

3.16 A major problem is the reluctance of the public sector to share data with consent; all the other forms of data sharing can broadly be done, with or without a specific statute. Legislation spells out what sharing is permitted, but less so what is required. Part of the issue appeared to be a lack of will by public sector workers to share data, either because of inertia or genuine worries about the Data Protection Act (as opposed to hiding behind it).

3.17 The mechanics of implementing data sharing had to be seen from the point of view of the data controller. For example, if the National Identity Number or DWP databases were made available through common access, how would the data owners handle the many requests for data that would be generated, and ensure that the data requesters are bona fide organisations, and were accessing the data for valid purposes? But if Government were to require this, *it would be done*.

3.18 The NHS shares data using a unique number; the problem for other sectors would be the greater number of people requesting access, and the lack of perception of a clear benefit to the organisation or citizen. The group therefore agreed to draft a EURIM paper that would document the different approaches to, and definitions of, data sharing. The paper would stress the public good (as opposed to the 'big brother' scenario), and would link the failure to share data with the consequent loss of benefits to the individual and cost to Government. The intended target would be Ian Watmore, and the group might also consider producing a briefing or report for parliamentarians.

3.19 Federation puts the access controls into the hands of the individual, balancing privacy against unauthorised or unnecessary access. In a consent-based system, an intermediary would effectively hold consent on behalf of the individual, but establishing an intermediary would require winning the trust of both the individual and the service provider. In banking, Experian and Equifax provide a service with the consent and goodwill of the individual. Perhaps we should be looking at a system in which consent can be similarly stored, with both individuals and organisations willing to use it? A possible route would be to get this on the agendas of Cabinet Office, Treasury or Ian Watmore.

3.20 Opposition to data sharing appeared to be propagated in large part from a social environment in which intellectual opinion and cultural attitudes were based on a distrust of Government; there appeared to be little appreciation in these circles of the possibility that data sharing is intended to improve service delivery to the citizen, and to protect the law-abiding majority against criminal activity and terrorism. We need to counter this atmosphere of negative thinking. At the BCS event on 1 December, Ian Watmore advocated the use of trusted intermediaries as one means of implementing the Government top priority of transforming service delivery in the public sector: the trusted intermediary model would thus appear to offer real possibilities for the subgroup.

3.21 It was agreed to hold a workshop on the afternoon of 13 January, at which subgroup members will bring their models to the table. A deliverable will be the integration of 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. This model would be refined in subsequent workshops and a prototype presented to Ian Watmore. It was agreed that IC² as a certifier of IT security professionals, could have a crucial role in reviewing and propagating the eventual model.

3.22 The lack of an effective model may not be the only barrier to public sector data sharing, and so the group should plan parallel exercises to counter the inertia associated with data sharing. A federated solution might help counter distrust of the single-relationship with the public sector, although a recent survey found that although people do not trust Government to keep their personal information secure, but they do not care anyway!

3.23 What corporate responsibilities and liabilities would ensue if data sharing were enabled? Would an individual be able to make one disclosure application under data protection rules – and obtain a copy of all government data held on him? Or would he have to make tens of applications to various arms of government which hold data on him? In a recent case, DWP was found liable because one part of it was given updated information about a claimant but did not share it with the rest of DWP – leading to arrest and false accusations of fraud. This could become complex across government and agencies if data sharing is also interpreted as placing an obligation on collectively updating information. This brings into focus what is meant by an organisation; data propagation should take the form of a formal transaction in order to establish where ownership and liability lie.

3.24 How might the Office of the Information Commissioner react if Government tried to make a registry under the DPA at a much broader level to facilitate data sharing? The Information Commissioner Richard Thomas had stated that the ID card proposals implied a complete change in the relationship between the citizen and the public sector. Although the ICO has said it is aware of the advantages and disadvantages in a consent-based model, and although it would advise on data protection issues, it would not actively support the model. In other EU countries, the ICO equivalent is more proactive.

4. Actions agreed

4.1 It was agreed that at the next meeting, specific members of the subgroup will each present a talk on a data sharing model; each talk will be a maximum of 15 minutes. It was further agreed that the speakers will email digital copies of their talks to Dave Wright by the first week in January 2005, for circulation to the subgroup prior to the workshop. In addition, there will be a summary of the DCA data sharing guidance. The aim is to present a succinct description of the different models, and the lowest common denominator technology model by which trust can be shared between various agencies that need to access the data. Recommendations on the way forward, and a draft briefing, would ensue.

4.2 DW undertook to contact Andrew Stott (Deputy CIO and Head of Service Transformation, E-Government Unit) with a view to alerting him to the EURIM initiative. The aim is to have a consensus of what the problem is, and to offer a solution in association with DCA, which may be multi-component.

5 Date of next meetings

5.1 It was agreed to hold 2 separate workshops on the afternoons of 13 and 20 January 2005, each of 4 hours duration.