

Theme/WP: E-Crime/Personal Identity

Drafted by: Dave Wright and Philip Virgo

Date prepared: 30/10/04

Date finalised: 31/10/04

Circulation: Group Members

Attached documents: 'Exemptions' for Process Map;

Powerpoint presentations on risk assessment, 'Headstart' talk & Models for Data Sharing

THE EUROPEAN
INFORMATION
SOCIETY GROUP

EURIM



Summary report of the Personal Identity Group meeting on Data Sharing, held in Room 4, Westminster Hall, 1000 – 1200 hours, Thursday 28 October 2004

Chair: Jim Lound (Experian);

Rapporteur: Dave Wright (EURIM)

SUMMARY OF MAIN POINTS

1. A press launch is planned for the two status reports produced by the Personal Identity Group:
 - 'Citizen or Subject – How far do we Control our own Identities?'
 - 'Data Sharing and Matching – the Law in Practice'

The press launch will focus on the Group's forward programme rather than past achievements. Personal identity and data sharing are at the heart of Government policy for implementing the Modernising Government programme, the Gershon efficiency review, and also for the e-commerce and e-crime agendas. Work in this area has been agreed by EURIM Council as one of its two priorities for the next 6 months.

2. Material from the status reports was submitted to the manifesto teams of the main political parties, and incorporated into the EURIM document 'Points for your Manifesto', which has been well received.
3. Discussions are being held with the Conference of Heads and Professors of Computing (CHPC), to explore the possibility of running a pilot scheme using the 'Circle of Trust' model to bring together university alumni and workforce updating programmes with the inclusion of validated CV services with access for prospective employers. The scheme will require identity checking and access permission routines which Experian is well placed to manage. It was agreed to produce a short proposal in consultation with the CHPC.
4. Work on the process map for data sharing had been limited by lack of responses, although a draft, incomplete chart was presented to the meeting on matching exemptions. The chart may be made available to members with the clear proviso that this is a draft for discussion only; gaps and errors could be filled and corrected over time. The Information Commissioner's Office offered the assistance in constructing the chart.
5. It was agreed to approach contacts in the financial and retail sectors to scope the nature of the risk assessment study, exploit current research and to plan what areas to focus on.
6. Home Office announced that plans to combine the proposed compulsory national identity card with passports and driving licences had been scrapped in favour of a stand-alone ID card. HO plans a new Whitehall executive agency to run the ID card scheme, a more secure online verification system to guard against fraud, and has decided to drop plans to set up a rival 'citizens' information project' population database.
7. The next step in considering a call for primary legislation for data sharing will be to scope forward actions in consultation with key contacts with the responsibility to deliver services. Key issues are to define the meaning of the terms 'consent-driven' and 'democratically accountable governance'. We also need to identify the points of leverage, who to work with, and how to motivate partners to make the changes happen.

1. Introduction and Objectives

1.1 The purpose of the meeting was to review progress of the various personal identity initiatives, and to plan a forward programme for the Group. Past work and achievements of the group had produced a number of potential workstreams, and these would be assessed during the meeting.

2. Press launch of status reports

2.1 Two recent status reports had been produced by the Personal Identity Group:

- 'Citizen or Subject – How far do we Control our own Identities?'
- 'Data Sharing and Matching – the Law in Practice'

The reports, available on the EURIM website, are ready for official publication, perhaps accompanied by a high profile press launch (subject to available budget).

Any press launch will focus on the Group's forward programme rather than past achievements. Personal identity and data sharing are at the heart of Government policy for implementing the Modernising Government programme, the Gershon efficiency review, and also for the e-commerce and e-crime agendas. Work in this area has therefore been agreed by EURIM Council as one of its two priorities for the next 6 months.

2.2 Material from the two status reports was submitted to the manifesto teams of the main political parties, and incorporated into the EURIM document 'Points for your Manifesto', which had been well received. No-one else appeared to be engaged in drawing together the various component threads on information governance in a coherent manner, especially in the public sector, where the biggest problems are encountered.

2.3 A number of issues from the 'Points for your Manifesto' document had been incorporated in a 'special report' article for 'Computing', authored by the EURIM General Secretary and presented to the meeting as a hand-out (see Appendix 1). He also referred to a hand-out of 6 key slides he would be using in a presentation next week for the CBI, on secure data sharing, which used extracts from the 2 status reports of the Personal Identity Group (see 'Headstar' document attached to email). More questions were posed than answers provided, and at the press launch of the forward programme the group will be able to refer to its recent achievements and outline its aims to build on these in a quest for practical solutions over a particular timescale, identifying the various partners with whom it will be working.

2.4 A date for the press launch would be selected in consultation with the EURIM Chairman, interested partners and representative technical press. Any members wishing to provide constructive quotes or other support would be most welcome to attend.

3. Formation of working group for the 'Circle of Trust' model

3.1 The previous meeting had called for the establishment of a working group to work with a Government Department to consider how to implement a practical solution around the 'Circle of Trust' model for identity management and data sharing. This would be driven by informed consent of the customer/citizen where possible, and in the public sector by statute and regulation where necessary.

3.2 DWP may be less receptive to approaches to trial the model, because they had an overriding priority as a service provider in delivering to citizens, and would probably wish to avoid any distraction. The need therefore is to identify a potential partner for testing and refining the model.

3.3 Edentity has been looking at how to take forward the education agenda with the e-Government Unit, though the 'Circle of Trust' model had not so far been considered. The group had no requirement for a commitment to adopt the model in an operational environment, rather it was looking for an opportunity to explore how the process could work. JISC (Joint Information Systems Committee) and BECTA (British Educational Communications and Technology Agency) are the two DfES agencies dealing with IT infrastructure in the education sector (higher and secondary education respectively). Edentity is deeply involved in talks with JISC, BECTA and academics looking at web services for effective, validated learning, and a deliverable is to produce a secure e-portfolio.

3.4 Another approach is through EURIM discussions with the Conference of Heads and Professors of Computing (CHPC), some of whose members sit on the relevant JISC and BECTA committees. The

aim is to organise a pilot service with a small number of interested heads of departments and large employers, to try to bring together university alumni and workforce updating programmes with the inclusion of validated CV services with access for prospective employers. The scheme will require identity checking and access permission routines. Experian would be well placed to help run a pilot scheme using the 'Circle of Trust' model to manage access to the CV service, especially since one of the Nottingham Universities is a target participant. It is hoped that money generated for departments will enable the service to be grown, additionally selling places on existing courses, with the prospect of an international catchment area. **It was agreed to produce a proposal in consultation with CHPC.**

3.5 Reports from the Intellect ID Card seminar held two weeks ago suggest that EURIM is far ahead of the thinking that was presented during that session, as was PITO. Home Office was aware of EURIM's work.

3.6 A request from DfES to meet and discuss the EURIM PI Group forward agenda was reported – this would seem to offer an ideal opportunity to explore the potential for working with a Government Department as a partner in a pilot of the 'Circle of Trust' model. Several members expressed interest, and it was agreed to try to organize a meeting in mid-November.

4 Development of the data sharing process map

4.1 Requests for additional input to the vertical process flow chart presented to the last meeting had not produced supporting data, and so work on the map had been limited. The flow chart led the data controller through a series of questions designed to point ultimately to a decision on whether or not data could be shared, or where further guidance could be obtained.

4.2 A chart on data sharing and matching exemptions was presented to the meeting as a hand-out (please see 'Data Sharing Grid' attached with email). This dealt with the start of the process flow and the wide variety of exemptions that apply to the principles of data protection. The exemptions are then applied to every step of the process flow. Both requesting and providing data controllers are listed because different exemptions apply to each. The chart at present was however largely unfilled, because checks had to be made for accuracy. Interested members to provide feedback in response to the process flow circulated with the last report, and also to the chart to be circulated with the report of this meeting.

4.3 Circulation of such a chart should not cause concern provided that it was clearly labelled as a 'draft for discussion only'. This is a well-established routine within EURIM, and allowed circulation of a consultation or working document, with requests for input and reporting of any errors etc. In fact, Home Office had requested that EURIM post on its website the EURIM e-crime grid of initiatives, responsibilities and players, as a working document, because it is the only example of its type. This has been posted, but with the clear proviso that this is a draft for discussion only; gaps and errors will be filled and corrected over time.

4.4 **The Information Commissioner's Office offered assistance in helping to construct the chart.** It is important to apply concepts of fairness, reasonableness etc. There will be a number of vertical process flows in which decisions would be guided by reference to the DPA principles.

5. Progress of risk assessment exercise

5.1 One of the issues raised during debate over ID Cards and personal identity systems was that of liability. On 23rd September a sub-group met to discuss whether it would be practical to apply classical risk assessment methodologies to the issues and if so, how. The group began by considering a risk-assessment exercise on the Personal Identity 'Circle of Trust' model used in the financial services sector. In documenting and assessing risks, costs and liabilities, the group is beginning a value/benefits analysis which, when extrapolated to all parties (individual, organisations, State) should help decide how the model might be used more widely in the public and private sectors. A major aim is to evaluate likely levels of false positives and false negatives generated by an authenticating system or by deliberate falsification of biometric data, and the impact of this on risk assessment. Results will be available for early input into any consultation on primary legislation for data sharing.

5.2 The exercise depended on 2 assumptions: that ID cards would be rolled out and that the intellectual capital generated by the risk assessment exercise would add to the 'circle of trust' model

objectives. There is also a possibility that people will not trust the ID card when it is available, and may use other forms of identification.

5.3 A presentation was given on combining risk assessment and scenario planning with financial modelling for business cases (please see 'RA Scenario planning' document attached to email). A major aim is to document the consequences of identified scenarios and risks, and estimate the costs if the 'circle of trust' data-sharing model is implemented. A matrix of different options will become available that can be used to develop a business case. For example what is the cost to the banks or Experian if they are expected to manage the tokens in a scheme that addresses the issue of false positives and false negatives. Is there merit in alerting individuals to queries directed to their personal information? What is the cost of rectifying false information? Would simple annotation be an acceptable and effective alternative?

5.4 An alternative solution might be to have an 'exceptions' database containing false identities for reference in the early stages of establishing a customer relationship. The purpose of the technique is to identify options, and estimate the cost and timescale of delivering those options. Mistakes could also affect the database; we should define what we understand by e.g. identity theft. Conflicting data could also be a problem, particularly in the case of medical records, although there are a variety of support tools available that should help with data management and conflict resolution. However, such tools were not usually designed to handle very large volumes.

5.5 Scenario planning is very useful for predicting future events based on the present, and can incorporate sufficient flexibility to allow us to prepare for, and cost, almost any eventuality, and any response to it. For example, if we interrogate a token, how will this be done? Will it be done in real time? - by wireless? – how much information will be held on the token? What happens if the token is lost? - the token may be a valuable item if stolen. A range of solutions are possible.

5.6 We need to approach the retail sector in planning; a mix of communities might be involved, as represented perhaps by the Jericho Group – a group of some 20 major multinationals who are trying to re-specify how they handle security, and collectively pressurising their suppliers to provide appropriate products and services.

5.7 Some quite sophisticated risk assessment is practiced in the retail sector to combat fraud – should we tap into this potentially valuable research? Would the introduction of risk assessment add value to current practice, or simply add new risks? We should not become bogged down in too much detail. However, that the level of detail is under our control – it could be set at the most useful level for the circle of trust.

5.8 A point of leverage would be the banks, who understood risk assessment; several individuals might be approached on the issue of security. The group should make the approaches to plan what areas to focus on and to scope the nature of the risk assessment study as part of the forward progress for the group. **It was agreed to contact key personnel on this issue.**

5.9 A key objective was to get the concept of doing risk assessments into the public domain – where it is not done at present - and to use it to inform policy and decision making.

6. Implications of the HASC Report

6.1 Questions were asked about the ID card scheme. Home Office yesterday announced the scrapping of the plan to combine the proposed compulsory national identity card with passports and driving licences. Instead, there will be the introduction of a stand-alone ID card to be issued alongside passports and driving licences. HO plans a new Whitehall executive agency to run the ID card scheme, a more secure online verification system to guard against fraud, and has decided to drop plans to set up a rival 'citizens' information project' population database.

7. Call for primary legislation on data sharing

7.1 An action from the last meeting called on members to organise an exercise calling for primary legislation to enable consent driven data sharing under democratically accountable governance. In order to facilitate progress, a presentation was given on how key issues had been approached in the financial services sector and, by looking for parallels, how these might be applied to the public sector (please see 'Circle of Trust' document attached to email).

7.2 When a consumer applies for credit to a provider (Slide 1), they sign an application form to give consent to a process, including giving the approved credit provider appropriate access to the individual's credit data at a credit reference agency (Slide 2). A benefit of this exercise is exposing the frequency of searches being registered, which may indicate a problem. The credit provider can then provide the CRA with a monthly update on the conduct of the account.

7.3 The detail of the process was explained using the presentation slides for illustration; once data requests are validated, the CRA registers a search and notifies the consumer (Slide 5). The CRA processes the request and according to type and decides the appropriate level of data that can be accessed under the terms of reciprocity and compliance (Slide 8). If the CP makes the consumer an offer and it is accepted, an account is set up which is updated regularly. This allows the system to react when a known fraudster move into a property and tries to utilise incoming mail in the name of the previous occupant.

7.4 A consumer can apply for a copy of their credit file at any stage through the CCA, once the identity of the applicant has been authenticated (Slide 11). Disputed data can be resolved through interactions between the agencies in the circle of trust, and the file is annotated and updated if necessary during this process (Slides 12, 13). The procedures, regulatory and legislative controls, historic issues, drivers and solutions were summarized, ending with a list of the differences between the private and public sectors (Slides 14-24).

7.5 On the issue of consent, from the DCA's point of view, the concept that of consent is irrelevant: either departments have the *power* to collect and share data, or they do not! Any change to this situation would almost certainly require primary legislation. Recent experience with the RIPA showed that the departments that signed up to it did so only in respect of communications data. This has created a situation in which departments can only demand data through specific routines and authorised personnel who have been trained in the required procedures. The consequences of this model have been a significant fall in requests for communications data.

7.6 The next step in considering a call for primary legislation should be to scope forward actions. This was agreed; key people to approach would be the Head of the e-Government Unit Ian Watmore, and the chain of CIOs charged with implementing good practice. The lead department for any generic legislation is the DCA, but currently in most areas it is departmental legislation that sets out the powers and routines for data sharing.

7.7 The lack of coherence in structures and in governance for sharing data is a profound weakness in the system, requiring or allowing non-compliance and threatening to undermine the whole modernising government agenda. Without change to promote data sharing and joined up government, the Gershon (or James) agenda cannot be delivered; massive pressure is thus building to demand both citizen-centric, joined up government and confidence in the governance of data sharing.

7.8 The group needs to work out how to take this forward. Key issues are to define the meaning of 'consent-driven' and 'democratically accountable governance'. We also need to identify the points of leverage, who to work with, and how to motivate partners to make the changes happen. We should also plan how to create 'win-win' scenarios for the DCA and eGU, and bring together the key parties, looking at the responsibilities of e.g. Ian Watmore and Minister of State for the Cabinet Office Ruth Kelly (including social inclusion issues). OGC should be involved because the driving force behind the demand for change is the Treasury, where Stephen Timms has the remit, supported by Ian Stewart MP, who chairs the EURIM Content and Issues Panel. This should allow us to set the terms of reference for an exercise.

8. Date of next meeting

8.1 The date of the next meeting of the full Personal Identity Group is planned for 12 January 2005, when it would consider the reports of the various subgroups charged with actions on:

- the circle of trust model,
- the risk assessment exercise,
- the process map, and
- the call for primary legislation.

8.2 The meeting closed at 1200.

APPENDIX 1

Building Confidence in the Delivery of Modernised Government

The effective use of ICT to transform the delivery of public services is central to achieving government objectives on health, education and law and order. But does the public believe government and its suppliers can deliver? We appear stuck in a twenty year cycle of bad practice: driven by political demands for "big pictures" and suppliers needs for big contracts to cover the cost of selling to government: the Minister announces a programme to transform the service, then comes a long and expensive consultancy exercise involving large numbers of "experts" but rarely front line staff (too busy fire-fighting) or customers (too difficult to get a valid cross-section). This is followed by an equally expensive (time as well as money) procurement exercise. The programme is then late, crippled by compromise and probably doomed, before implementation begins.

The private sector has long used variations on "structured evolution": step-by-step change within an overall strategy, each step separately justified (including the use of internal and external market research to check requirements), implemented with competing suppliers forced to interoperate and regularly assessed. The pieces are in place for government to do likewise: Gateway Review process, e-Gif standards and Framework Contracts. But most of Whitehall still appears stuck in a centralised, command and control time-warp. The solution is to apply private sector disciplines, with rolling programmes of reform: thinking big (basic principles and interoperability frameworks), starting small (departmental and agencies' experiments) and building on success (scaling and linking that which works).

Recommendations

* All central government programmes should pass through the full Gateway process with the comments on those which go forward made available to the National Audit Office and Public Accounts Committee. There is a balance to be struck between the confidentiality necessary for effective peer review and the need for accountability when professional judgement is overridden by political expediency.

* Require details of winning bids, including performance monitoring and change control processes, to be placed in the public domain unless they really do affect national security. The collapse of public confidence means that any case for confidentiality must be balanced against the need to avoid allegations that it serves to conceal incompetence, inefficiency and corruption. The Freedom of Information Act provides the necessary framework and guidance has already been drafted by the Office of the Information Commissioner.

* Ensure proper career paths, reward and governance structures for the public servants whose competence and integrity, intellectual as well financial, is central to the successful running of Great Britain. All political decisions should be properly recorded and the recommendations of the Select Committee on Public Administration for a Civil Service Act should be carried forward (with due consideration for the concerns in the Minority report). Similar governance routines to those for public servants should apply to all those contracted to help undertake statutory functions.

Removing the Barriers to joined-up government

The main obstacles are cultural but these are reinforced by legacy legislation that prevents data from being shared between functions and departments, whether or not the citizen requests it. A classic example is family tax credits: claimants required to repeat information on their tax returns, in a different format, doing the calculations themselves. Most gave up or did it wrong. There was no option to request the Inland Revenue to use the data already on file.

There is a parallel tangled web of powers to demand customer information from business for regulatory and investigatory purposes. The governance of publicly held information is equally

confused, with vetting and draconian penalties for abuse by (for example) the staff of Royal Mail or the Inland Revenue, but not for the staff of those contractors who run outsourced call centres and enter or access sensitive data for many central and local government departments and agencies.

The sorry state of affairs revealed by the Bichard enquiry is repeated across much of Central and Local Government and lies behind public views on ID Cards, particularly the scepticism that these will be anything more than another spectacular waste of public money. It is also the prime obstacle to delivery of the efficiency agendas shared by both Government and Opposition.

Recommendations

- * Enable departments and agencies to adopt consent driven routines, including validation routines, akin to those for the files of the credit reference agencies and financial services sector, while retaining default powers (under clear third party governance) to demand access for emergency or enforcement purposes.
- * Extend the third party governance and mandatory training principles in the Regulation of Investigatory Powers legislation to cover all statutory powers to demand information from business or the public.
- * Provide clear guidance for all those handling public sector personal information as to with whom it is to be shared with, under what circumstances and how to check their identity/authority – such guidance is also needed by those in the private sector from whom information may be required under statutory powers.
- * Introduce graded and publicised penalties for personal or organisational abuse, from individuals accessing or amending files to aid impersonation, fraud or blackmail to organised abuse down to “mere” bad practice and lack of adequate guidance and procedures.
- * Assess the risks and liabilities entailed with the various trust and governance models (current and proposed), how these vary with changing business requirements and technical processes and the effects of volume and required response time.
- * Provide rolling departmental programmes of file cleaning and validation, these should not be one-off exercises and will not be cheap, but costs will fall as files and processes are brought together over time.
- * Put in place an overarching strategy for ensuring that the growing number of personal identity related initiatives (public and private) gives additional protection and not merely dis-economies of scale or an expensive and a wasteful illusion of protection.

Those interested in helping turn such recommendations into action should visit www.eurim.org.uk for details of our work on Personal Identity and Data Sharing .

Philip Virgo, Secretary General, EURIM