e-Infrastructures for Identity Management and Data Sharing: Perspectives across the Public Sector

Mary Rundle

Fellow, Berkman Center for Internet & Society (Harvard Law School)
Non-Resident Fellow, Center for Internet and Society (Stanford Law School)

Visiting Fellow, Oxford Internet Institute, Oxford University

A strategy forum organized by the Oxford Internet Institute (OII), University of Oxford, with the support of the Office of the Information Commissioner, the Joint Information Systems Committee (JISC) and the Cyber Security Knowledge Transfer Network (an initiative of the Department of Business, Enterprise, and Regulatory Reform).

The Forum was held on 7-8 June, 2007.

1. Executive Summary 2
2. Background to the Forum 4
3. Requirements of Distinct Departments and Levels of Government 6
4. Case Study: Identity Management Across Public-Sector Organizations 9
5. The National Identity Card 10
6. Three Technical Models 11
7. Avoiding Function Creep 13
8. Who Decides 16
9. Public Attitudes and Trust 18
10. The Public-Private Partnership in Covering Costs 21
11. Pilot Project in the Education Sector 23
12. Conclusion 25

1. Executive Summary

The OII strategy forum 'e-Infrastructures for Identity Management and Data Sharing: Perspectives across the Public Sector' was organized to allow the UK public sector to explore how to take advantage of innovations in digital identity management and data sharing. New technologies could help public-sector organizations to identify citizens in ways that enhanced their personal privacy and built confidence in government services; to share relevant data for personalized and interconnected services and fraud reduction; and to enable authentication for different types of transactions. Could an identity infrastructure become a shared service for use across sectors, operating in a simple and secure manner and protecting the privacy of personal information?

The group considered challenges from a public-sector practitioner's point of view. In education, people could have educational records accessible through digital identities tailored to that purpose. In transport, people would interact with a system that actively collected personal data (e.g., residence and banking information). The Department of Work and Pensions was working on a 'change of circumstances' mechanism to give citizens a single point of contact any time they needed to change information; customer data could help predict future outlays. Local government aimed to have a relationship with citizens, serving them in line with the democratic process as they accessed services; dynamics among government levels could be analogous to those that would apply if an international identity infrastructure emerged.

In considering how common identity management solutions could be implemented across public-sector organizations to bring increased functionality, the group took up a case study on agencies involved in the death and bereavement process, which highlighted: the need for streamlining, gradations in the need for detail, differences in

the need for data quality and certainty (risk management), different points of control, and legal checks on data sharing.

The group generally agreed that people needed a secure method of identification vis-à-vis government in order to access public services. However, this simple proposition pointed to more challenging questions, such as: Should there be a general identifier? Would the identifier be linked to databases? Who could access them? What was the grand scheme across government? How were lines drawn for information sharing among agencies, and where did permissions stop? What were the mechanisms for accountability? How could decision-makers give citizens an effective consenting right in the treatment of personal data?

For a national identity card, a key question was *how such a card would be put to use*. It would be poor policy to require people to use the card to access services. Biometrics could serve as part of 'local' authentication, but they should not be stored in databases. Making these matters urgent was the fact that the Home Office expected to have a full identity card scheme in place within 10 years.

Despite looming deadlines and the need to incorporate legacy systems, policymakers were open to broadening their inquiry as to what different technologies offered. Different technical models offered different capabilities. One model, referred to as 'organization centric,' entailed cross-domain identity management, for example allowing different sub-sectors of public administration to synch up identifiers. Another model, the 'federation' or 'federated' approach, involved the linking of accounts by an identity provider in the service of organizations in a circle of trust. With the 'user-centric' model, the individual was the one who kept the accounts and was the only party who knew the links between them. The models could emulate the complex levels of disclosure that existed in the real world. In different combinations, the models could offer a continuum of choices to suit various information-sharing needs and data protection requirements.

Still, in the name of efficiency and security, government organizations might be tempted to access and share data beyond original expectations. Data protection principles served as a legal check on data sharing and function creep. Identity management technologies offered mechanisms for parties to meet data protection requirements. A possible approach would be to prevent linkage between data describing an individual's characteristics or actions, and data defining that person's absolute identity. Anonymity, which was desirable in many contexts, might at first glance seem to thwart auditability; technologies were available to address this apparent tension. Was a cross-domain (and cross-jurisdictional) audit trail needed?

Participants disagreed as to who should be granting whom the right to control data. Private sector experience showed that users did not want one large entity to be at the centre of all their data and relationships and everyone else's as well. Since it was generally agreed that people had a natural role in managing certain data pertaining to them, perhaps the three technical models could be used in combination according to different needs.

Besides feeling comfortable with the technology itself, the public also needed to have trust in government as it operated identity systems. Accountability to citizens should be a primary concern since an important aspect of citizenship was a person's ability to scrutinize what government was doing. Thus, the public should be able to measure how the system was operating. The identity infrastructure should support best practices in data protection.

Public-private partnerships could help bring investment in and drive uptake of an identity infrastructure. To what degree should the public sector lead? The orientation should not be to roll out a master plan, but instead to ensure flexibility and migration capabilities since technology and public policy were apt to evolve.

The group then considered the promise of the education sector for a pilot project, which stood out because: its young population would find the technology easy to use; education could be viewed as a 'friendly' pilot project as data concerned people's achievements; this pilot could support the agenda of instituting an identity management system that would follow a person throughout their life; and, finally, education could help bring acceptance of a cross-jurisdictional identity infrastructure.

2. Background to the Forum

By way of context, this forum recognized that identity management[1] and data sharing were key issues in digital networking innovations in public services across the United Kingdom (UK) and worldwide. These issues required public sector organizations to seek appropriate approaches that:

- Identified citizens in ways that enhanced their personal privacy and built confidence in government services.
- Shared relevant data in order to deliver more personalized and interconnected services while reducing the potential for fraud.
- Enabled authentication at a level sufficient for any particular service or transaction, many of which might not require personal identification.

[1] As noted by Jonathan Bamford, Assistant Information Commissioner: 'Though 'identity management' is a term that has become widely used, it is not clear whether it has a commonly accepted meaning.' Many viewed it as 'streamlining the processes and systems needed to verify identity for any number of remote transactions,' and 'providing a more efficient service to customers and making better use of the information already available through reliable linkage.' Jonathan Bamford, 'Identity Management: Achieving Data Protection Compliance and Inspiring Public Confidence,' Position Paper for the forum on e-Infrastructures for Identity Management and Data Sharing.

Different sectors in the UK had set about addressing these challenges to meet their own particular needs, resulting in a growing range of methods and initiatives and an accumulation of experience and lessons learned. The following table illustrates a few of these efforts.

Education	UK Access Management Federation (providing single online sign-on access within or across organizational boundaries)
Local Government	Government Connects; various local smart card schemes
The National Health Service	The NHS number; Connecting for Health; smart cards issued to professionals for IT systems access
Central Government	The Identity Card; Government Gateway; extensive data sharing across the main databases
Banking and finance	Chip and PIN cards; credit reference databases; bank experiments with One Time Password (OTP); devices for online authentication
Mobile telephones	Mobile phones as a potential secondary factor for authentication

One strength in the kinds of methods and initiatives mentioned in the above table had been the development of new technologies, open-standards and 'user-centric' identity management strategies. However, there had been a lack of sufficient dialogue between the various sectors in this field of identity management and data sharing to explore fully key questions such as: (a) was it time to consolidate around a common set of methods that are developing a proven track-record in specific sectors, or was it too early, given emerging technologies? *and* (b) as every sub-sector of public administration serves parts of the same population, could the cumulative experience for individuals be improved by reducing the number of approaches used in the public sector?

The Oxford Internet Institute (OII), with the support of the Joint Information Systems Committee (JISC) and Office of the Information Commissioner, organized the forum to provide an opportunity to identify common identity management requirements of public sector agencies. A main point of inquiry was the possibility of an identity infrastructure becoming *a shared service* for use across sectors, in a way that would operate in a simple and secure manner and that would necessarily protect the privacy of personal information.

By hosting this forum on e-Infrastructures for Identity Management and Data Sharing, the organizers' intention was to help move towards a common vision of what government agencies saw as an appropriate identity management and data sharing infrastructure, and of how actors in the UK could take steps towards it. At a later stage, it might be appropriate to hold a follow-up event, in which a proposed 'public-sector' view would be discussed with commercial stakeholders, such as the banks and mobile network operators, as well as civil society actors.

The forum's organizers invited senior-level individuals who were known to be responsible for the policy and practice of identity management and data sharing, in order to offer a neutral ground to discuss related issues in the public sector. The

numbers were limited to promote free-flowing dialogue, with all participants around one table.

The organizers hoped that all parts of the public sector would be represented, but they gave particular weight to education as this area offered particular opportunities for innovation. There were also experts in identity management from the academic and business worlds who were aware of the significant UK and international initiatives in this field. As discussion was subject to the Chatham House Rule, this report was drafted so as not to attribute comments to individuals unless they granted specific permission to do so.

3. Requirements of Distinct Departments and Levels of Government

As the group teased out needs and concerns of different departments and agencies at different levels of government, a common theme was the fact that each faced limits on decision-making, due to (a) departmental legacies, and (b) the momentum of current policies, such as national identity cards. These factors were said to affect their ability to be free-thinking in visions of a desirable model for the future.

The group considered the main challenges from a practitioner's point of view in the public sector, taking different departments in the UK as examples, and also considering the roles of local versus central government.

Education

The orientation of the Department for Children, Schools, and Families (DCSF, formerly the Department for Education and Skills) was toward providing benefits to customers rather than toward exerting control. Because the services provided were free, fraud was scarcely a problem; the agency therefore had to be careful not to scare people off by asking for identity information since there was not an obvious need for it. The agency needed to communicate that, by knowing who its customers were, it could offer personalized services (delivering educational services specific to the person online, etc.). The agency was doing a scoping exercise to determine what its objectives were, and where it made sense to link information. Results were pointing to an approach where a person would have one unique identifier for the education sector since there was little cause for a person to use different identifiers. In working closely with the Home Office for the past year or so, officials from the DCSF had been making the case that this agency's needs were different from those of other government agencies.

In terms of the specific process, a new applicant would be given one number to use when submitting all applications henceforth; if the person were unsuccessful one year, they could apply again, with the same information on file. The data would follow students through different phases to enable the tracking of educational status over time.

Higher education had a fairly homogeneous culture throughout, which allowed a certain standardization within contexts.

With respect to the treatment of information relating to minors, officials were contemplating a post age-14 system, but at the same time they wanted to roll this limit back to an earlier age so that more information would be tied together. However, it seemed people were cautious about using one unique identifier throughout their educational experiences; and in terms of the identity information contained in the system, it seemed certain information, such as what a person did in kindergarten, should be expunged after a period.

Transport

The personal information that the Department for Transport (DfT) wanted to use was not unlike what other government agencies sought. The primary difference was that people would soon be *forced* to use a service and to pay for it (as opposed to the current arrangement in which they did not have to interact much with the system and drove on the roads for free); in addition, the DfT would be actively collecting personal data. For example, people would have to submit residence information if they wished to benefit from cheaper rates, and payment would require banking information. The Department was exploring satellite-based road pricing.

The Department observed a see-saw balance between privacy and efficiency. It had many questions about appropriate privacy approaches, but few complete answers as of yet. Meanwhile, many citizens were worried that location record would be passed on and used for other purposes.

According to Richard Weider,[2] to allay these concerns the DfT was 'taking account of data protection and privacy as key issues' in its Demonstrations Project and in its work with local authorities. He indicated that road pricing schemes would 'follow existing and future legislation on the use of personal information collected.'[3]

Pensions

The Department for Work and Pensions (DWP) last year had been asked to look at 'change of circumstances' so that citizens could have one point of contact any time they needed to change information. On one level, the Department needed a single, standard, trusted method for confirming someone's identity, and this method had to work across government agencies that would need not just to confirm and share the information, but also to limit this sharing to appropriate points of the governmental system only. The system should work over 3G, text and other technologies. On another level, the Department was looking at how it might use customer information to be more *predictive* about an individual's expected benefits. This predictive capability would improve budgetary projections for planning purposes, and it would also reduce hassles for people whose circumstances were changing since the agency would already have relevant information on hand (e.g., to allow automatic payments to go out without a person's having to apply).

The agency did not experience much identity fraud in its system. Its challenge was that the Identity and Passport Service had been given the remit to base the national identity card on the DWP's database. The problem was that designers could not start from scratch – the current database system preordained many of the parameters of the national identity register.

---

[2] Richard Weider is Road Pricing Policy Adviser for the Department for Transport.
[3] Richard Weidner, Position Paper for the forum on e-Infrastructures for Identity Management and Data Sharing.

Local versus central government

Local government could be seen as bundles of services sitting on top of what was essentially a corporate structure.

A local government body aimed to have a relationship with citizens, whom it was responsible for supporting through the democratic process. People would need to access services through local agencies that they trusted. The individual, it seemed, should naturally have a seat at the table.

Local government might partner with central government, private sector actors like mobile phone providers, or other entities to allow citizens to access services easily.

Meanwhile, there were mandates, and certain infrastructures had to be accommodated despite the fact that it was unclear how costs would be covered. Local and central government did not always enjoy a cosy relationship, and friction often stemmed from budgetary concerns. Some were of the view that, if local authorities had systems that were up to scratch with certain standards, the central government should accept those systems. Today, for example, different regions had different practices for the enrolment of a person's information as they established an identifier.

In some ways the central government's push for identity management seemed to go against trends: In other contexts the last 10 years had brought a big push to devolve government to the local level. This push for conformity with central systems seemed to go against the flow.

Adding complexity to the dilemmas of government levels was the fact that there was an international aspect to agencies' work. Systems often had to work across national jurisdictions. These jurisdictional issues could arise with the most basic identity information. For example, across EU Member States, authorities needed to accept as valid each other's systems for dealing with birth dates. So, too, in the field of education, institutions often operated as international organizations, but the government agencies making decisions about identity management systems often were thinking in terms of just one country.

It was suggested that the Government Gateway and the Government Secure Intranet both provided a ready mechanism for interaction between local and central governments. After all, through trusted party tools, central government agencies had been able to have functions extend to visa offices abroad, which were able to handle biometrics and other information. This smooth interaction among agencies was helpful to the private sector as well, since employers no longer had to do the verification work for employees and such.

Still, the question remained: How were local authorities to make sense of all the relevant factors and meet deadlines for having systems in place? In seeking to do so, they had to bear in mind their primary job – namely, to act in the interest of the public and build systems that respect the democratic process by ensuring an informed and open public debate.

4. Case Study: Identity Management Across Public-Sector Organizations

In considering how common identity management solutions could be implemented across public-sector organizations to bring increased functionality, the group took up a case study on agencies involved in the death and bereavement process, using as its basis a report published by the HM Treasury Office in 2006.[4] The report told the story of a person who had lost a parent and who then had to interact with over 40 different government agencies in order to resolve all the formalities surrounding the death. It illustrated the concept of Joined-Up Government (JUG), which had been fashionable in policy circles two or three years earlier, as well as the newer notion of 'citizen-centric' government, which rested on JUG.

Discussion of the death and bereavement case study highlighted the following lessons for planning public identity management systems:

- *The need for streamlining* – There was a good deal of repetition in processes as many agencies that should have had access to information either did not have it or did not trust its reliability.

- *Gradations in the need for detail* – The amount of detail needed in identity information differed by agency or task.

- *Differences in the need for data quality and certainty (risk management)* – Different agencies and tasks had different requirements for data quality, and the acceptable level of risk regarding data reliability varied accordingly. It was important not to take data collected for a purpose in which poor data quality was tolerable, and then to introduce that same data elsewhere for a purpose requiring higher quality.[5] In other words, where it made sense to let information flow, agencies had to ensure the quality of data.

- *Different points of control* – The death and bereavement case illustrated that there were situations when it made sense for government to be able to match up data (e.g., one agency passing a death certificate to another to enable burial arrangements); there were others when it made sense for the user to choose whether to let data flow (e.g., sending out word that they would like to be contacted by a counselling centre for bereavement support).

- *Legal checks* – One legal aspect to information sharing was that an agency might not be authorized to deal with data if it came from another agency source, or to pass data to another entity. So, for example, an agency might be prohibited from providing information to an insurance company even if this sharing would facilitate the provision of services to

[4] Sir David Varney, 'Service transformation: A better service for citizens and businesses, a better deal for the taxpayer,' 2006. Available at: http://www.hm-treasury.gov.uk/media/4/F/pbr06_varney_review.pdf

[5] Of course, there were other concerns here as well, for example notice and consent in the purpose for which data was collected and subsequently used, if applicable.

> a person. The walls were there to protect privacy and prevent function creep.

By highlighting inefficiencies and inconveniences, the death and bereavement report was likely to spur policy changes in practices of the DWP (on whose system the Identity and Passport Services would base their systems), especially for a 'change of circumstance' situation; these same rationales might be cited for policy changes in other agency contexts as well.

5. The National Identity Card

Providing a backdrop to discussion on the national identity card were remarks the previous evening by Sir David Normington, Permanent Secretary of the Home Office.[6] Sir David indicated that the Whitehall Identity Strategy Group was intent on seeing the rollout of a cross-governmental approach to identity management. Stating that 'as citizens and consumers, we need to be able to assert and prove our identities with confidence,' he explained that the UK government's case for an identity scheme rested on the pursuit of security – which included fighting terrorism, illegal immigration, and fraud, as well as supporting vulnerable groups like the elderly and children.

The group generally agreed that people needed a secure method of identification vis-à-vis government in order to access public services such as social security, the tax system, and driver and vehicle licensing.[7] However, this simple proposition pointed to more challenging questions, such as: Should there be a general identifier? What might it be? Would there be an associated identification service? Would the identifier be linked to databases? Who could access them? What was the grand scheme across government? What about the notions of a data owner and data controller for accountability? How were lines drawn for information sharing among agencies, and where did permissions stop?

For a national identity card, a key question was how such a card would be put to use. A cryptographer in the group stressed that it would be very poor policy to require people to use a card containing a root identifier to access services.

In their quest to establish a secure method of identification, government agencies were now talking about collecting not just biographical information for government databases, but also biometric information. These moves seemed to be more about organizational convenience than citizen empowerment. How could decision-makers make citizens an intrinsic part of the equation, giving them an effective consenting right in the treatment of personal data?

---

[6] Sir David made these remarks at a public event hosted by OII on 'The Management of Identity and Personal Information on the Internet: Public and Private Initiatives for Addressing the Problems', June 7, 2007. He chairs the Whitehall Identity Strategy Group.

[7] Meanwhile, in private dealings, the myriad cultures interacting in different contexts might have their own preferred standards for assuring that a person was who they said they were. There was demand for community-based approaches to authentication, where a group of people could determine the degree of reliability required for authenticating within their group.

It was noted that databases were prone to being hacked, as no system was 100 per cent secure. Why, then, would society want biometrics to be stored in databases? (Disney World and car rental companies already were storing fingerprints.) Biometrics could have a role at the endpoint, as part of the 'local' authentication process – but there was no reason for this information to be stored away from the citizens, where it was not under their personal control.

If digitized biometrics were stored locally, and another unique identifier (say, a unique number) were issued to the person, then the two could both be referenced in an authentication process. Cryptography could prevent an entity from having access to them both, so that they could not be joined together. As explained by Jerry Fishenden of Microsoft, 'Meaningless but unique numbers (MBUNs) used in combination with a variety of authentication and identification techniques' could help protect privacy and security while 'still enabling operational efficiency.'[8]

The need to safeguard the security of biometrics was underscored by the fact that the government-authentication service would likely be tied into an international service: A global registry would check that a person had not previously registered and thereby prevent an individual from registering with multiple services. The global registry would not need to have any further involvement with the identity/attribute certificates that would be issued by other parties (in this case, national or local governments). Such a global service should be designed in a way that prevented linkages between a person and their characteristics.

Making these questions urgent was the fact that the Home Office expected to have a full identity card scheme in place within 10 years, and it planned to start issuing cards to the general public in 2009. The envisioned structure entailed a number of databases with access controls, rather than a single monster one. In other words, while there would be a central registry service for a person to be entered into the system, other personal data would be held in separate databases elsewhere. The identity card and passport services were to be based on what DWP already had in place because that approach was less expensive than other options and seemed to make sense. But policymakers were asking whether they would do better to think along broader lines. Were there different technical models that would allow them to do so?

6. Three Technical Models

The group differentiated among three main technical models for information sharing in digital identity management systems.[9] In very basic terms:

One model, referred to as 'organization centric,' entailed cross-domain identity management, where different entities synched up identifiers. Participating organizations created a central index, sometimes called an identity register, which was then used to match up an individual's records across those organizations'

[8] Jerry Fishenden, 'Identity Issues and Developments,' Position Paper for the forum on e-Infrastructures for Identity Management and Data Sharing.

[9] These three models developed as ways to move beyond the traditional 'silo' approach to identity management.

various databases.[10] This approach was essentially expanding the 'silo' where information was hoarded by an entity for its own benefit, so that entities together created super, shared accounts.

With the 'federation' or 'federated' model, service providers would form a 'circle of trust.' A user could access services within that circle by authenticating to a central 'identity provider,' which in turn would inform service providers about the authentication status of that user. The user could have different 'aliases' for each service provider, and the identity provider would then map these identities and relationships securely. The identity provider, however, would be serving on behalf of the service providers. (The idea here was to prevent fraud by users.) An agent of the central party kept the links and made the data flow correctly.[11]

Then there was the 'user-centric' model, where the individual user was the one who kept the accounts and was the only party who knew the links between them. The user could choose to employ different identity providers (sometimes called 'information brokers') to store and vouch for various sets of their identity information. It was not that identity claims were self-asserted, but rather that 'multi-party security' allowed a certain division of control between the organization and the user. Ideally, no linkages should be established, and the absolute minimal information would cross domains.[12] The user-centric approach recognized that a user had multiple, distinct relationships and should have a recurring consent role in any linking. The goal here was to allow the user to retain control – not just technologically (e.g., by using anonymous credentials to minimize the flow of personally identifiable information between actors), but also legally and socially.

It was noted that all three models could achieve 'single sign-on'[13] wherein the user was required to authenticate themself only once for multiple transactions; however, the models each carried different implications in terms of control over the sharing of information.

Identity was *contingent on relationships* in both the federated and user-centric models: In the absence of a relationship permitting the release of a person's identity information from the identity provider that stored it, to the service provider that sought it for a transaction, the user had no meaning to the service provider.[14]

The accepted wisdom in this area was changing from a sense that automation had to make things simple (e.g., via one identity) to the sense that technology could emulate the complex levels of disclosure that existed in the real world.

---

[10] John Harrison, 'Balancing the Approaches to Identity Management and Data Sharing,' Position Paper for the forum on e-Infrastructures for Identity Management and Data Sharing.
[11] Stefan Brands, 'The Management of Identity and Personal Information on the Internet: Public and Private Initiatives for Addressing the Problems,' Position Paper for the forum on e-Infrastructures for Identity Management and Data Sharing.
[12] New identity management tools were trying to address privacy issues, so that even if users had the impression that they were transferring the same information in transactions, technically the information sent to the parties receiving the data would be different each time. This cryptographic method would help prevent a linking of the data to create large profiles.
[13] Single sign-on and complexity in relationships concerned different aspects of an identity system.
[14] For the federated model, permission was determined among the circle of trust; for the user-centric model, permission was granted by the user or their agent.

Despite the attractiveness of having alternative models, the label 'user centric' could cause confusion and undermine that model's appeal; after all, each agency viewed its own approach as citizen-centric, regardless of the model it was pursuing. Although the term had originated to describe data flow architectures, it was increasingly borrowed by other models to communicate that the user was important. Perhaps 'multi-party cryptographic' would be a more useful term than 'user centric'.[15] Words mattered; they were political. Neutral terminology was needed.

For officials tasked with meeting mandated deadlines, the pressing challenge was to make sense of the different models and accompanying choices in a timescale that was useful.

7. Avoiding Function Creep

A temptation for government organizations, if they had access to data, would be to share it in a back room. The logic was that if information were readily available, why not make use of it and allow greater efficiencies? The problem was that such practices had the effect of expanding the reach of government through gradual function creep.

Data protection

Data protection principles in fact served as a legal check on function creep. An agency might not be permitted to deal with data from another agency source, or to pass data to another entity. The Information Commissioner's Office viewed identity management technologies as offering mechanisms for identity providers and service providers to meet data protection requirements, as they could help ensure that personal data was:

- processed fairly and that individuals understood how their information would be used;
- not excessive;
- adequate for its purpose;
- accurate and kept up to date;
- available to the individual that it was about; and
- held securely.[16]

[15] Even among specialists, different terms gave rise to varied interpretations, so work was underway in several groups to set out an ontology (that is, a commonly agreed set of terms for the range of concepts involved). Of course, the fact that similar work was being done in different settings could prove problematic.

[16] Jonathan Bamford, 'Identity Management: Achieving Data Protection Compliance and Inspiring Public Confidence,' Position Paper for the forum on e-Infrastructures for Identity Management and Data Sharing.

The Models

Because the structure of a system could enable or prevent this increased government access to and use of identity information, the technical models carried implications for function creep.

According to Stefan Brands, a core problem with an architecture having one central identity provider would be that it could 'electronically monitor all users across all services, in real time.' It was arguable that in Europe such an architecture would violate Article 8 of the European Convention on Human Rights, as any interference with privacy rights was to be as limited as possible. Brands asserted: 'As identity architects with a background in information security and privacy can attest, federated identity architectures violate this requirement' since 'far less intrusive means exist for achieving the objectives of single sign-on and data sharing.'[17] If adopted on a society-wide scale, an architecture with one central identity provider would not only be 'in conflict with the principles of data protection legislation,' but would also 'have unprecedented repercussions for civil liberties and democracy.' Problems would go well beyond privacy as the identity provider could 'selectively impersonate any user at any service provider' and could 'falsely deny access to any user'; it would also be 'a target for denial of service attacks.'[18]

It was suggested that the same pitfalls would be present in a user-centric architecture if the market led to a concentration in identity providers. Although the model offered the promise of decentralization, users simply might not bother to expend the effort to divide up their identities among different identity providers, and for their part, service providers might be willing to deal with only select identity providers whom they deemed reliable. The result could be that a limited number of identity providers would dominate the market, and this small set would then have access to vast amounts of personal data and could possibly misuse it. In other words, a concentrated market could lead to corruption, robbing users of the control over the treatment of their data that they had been promised. In this sense, the user-centric model's purportedly decentralized architecture would offer little advantage over models that explicitly had a centralized identity provider.

Separation of functions

As explained by Pete Bramhall, a good approach would be to break or never form the link between data describing an individual's characteristics (or his/her actions) and data defining that individual's absolute identity.[19] A variety of technical approaches could achieve this separation, ranging from (a) 'approaches in which all communication and interaction between digital service provider and consumer' were done 'on the basis of anonymous credentials', to (b) 'those in which the service provider's identity management systems' were 'designed to follow all the consumer's

[17] Based on this logic, parties could be viewed as having a pro-active responsibility to offer privacy enhancing technologies such as 'multi-party security' coupled with anonymizing tools such as those available through Credentica and IBM's Idemix.
[18] Stefan Brands, 'The Management of Identity and Personal Information on the Internet: Public and Private Initiatives for Addressing the Problems,' Position Paper for the forum on e-Infrastructures for Identity Management and Data Sharing.
[19] Pete Bramhall, Position Paper for the forum on e-Infrastructures for Identity Management and Data Sharing.

requirements regarding the management and governance of his/her identity information (and thus act as his/her proxy)' and were 'verified as actually doing so.'[20]

The UK's Government Gateway provided 'an information and identity broker that could be a key component in a national identity system,' doing so 'with due regard to the appropriate partitioning of identity contexts and information contexts.'[21]

Problems of anonymity

The user-centric model seemed to fit well with those government agencies whose default presumption was that the user should be anonymous while the agency accessed identity information on their behalf (for example, if identity management tools were used in voting). Some participants were concerned that anonymity was at odds with auditability. For example, at first glance it might seem problematic if a government enforcement agency wished to audit anonymous, user-centric transactions; after all, links would have been prevented and the user would be the only one to know that they were the person on that end of the transaction.[22] However, privacy and auditability did not necessarily conflict: There were many cryptographic schemes that could maintain the anonymity of users while allowing fraud to be detected and traced.[23]

Need for audits

Audits of service providers could be necessary to ensure they followed 'all the consumer's requirements regarding the management and governance of his/her identity information,' as Bramhall suggested.

Historically, audit trails had been within one domain only, but now audit trails were able to cross domains. Was a cross-domain audit trail needed, and, if so, what did it require? If an identity management system were used internationally, would it require international audit capabilities?

---

[20] Id.

[21] Jerry Fishenden, 'Identity Issues and Developments,' Position Paper for the forum on e-Infrastructures for Identity Management and Data Sharing.

[22] Both the individual and the service provider would know the transaction details, but the service provider would not be able to link the individual to any other transaction or legal identity.

[23] For an example of how privacy and auditability can simultaneously be designed into a system, see, e.g., Choi, J. Y., Jakobsson, M., and Wetzel, S., 'Balancing auditability and privacy in vehicular networks,' in Proceedings of the 1st ACM international Workshop on Quality of Service & Amp, Security in Wireless and Mobile Networks (Montreal, Quebec, Canada, October 2005), Q2SWinet '05, ACM Press, New York, NY, 79-87, at: http://www.cs.stevens.edu/~swetzel/publications/balancing.pdf

8. Who Decides

As a backdrop to the discussion on choosing among the different models, perspectives clashed as to *who should be granting whom the right to control data*.

Some felt that citizens should have no choice in matters where government agencies rightfully needed to share information for the sake of efficiency. This camp felt that data-sharing among organizations that were supposed to work together did not pose a problem. Questions of information sharing between local and central authorities would need to be worked out, but in any case it was up to the government to decide these matters. The government could offer citizens roles in choosing arrangements for additional services (e.g., insurance matters), and there would logically be exchanges which citizens should trigger themselves (e.g., choosing to avail themselves of services of a bereavement counselling centre). But the actual allocation of this decision-making power was the government's domain.

One participant expressed the view that, in recent months, the large majority of citizens had been hindered from having good service because a small minority of citizens had been objecting.

Others believed that what was important was that practices be clear and transparent to the public, and that policies result from public choice.

These divergent views on who should be granting whom the right to control data naturally corresponded to views on *who should determine which model was used*. Depending on the model(s) chosen, either the institution (in the case of organization-centric or federated models) or the user (in the case of a user-centric model) would control the release of data.

A non-user centric approach might rely on the moral contract a person had with their government. This was analogous to the military covenant, where the government promised to equip soldiers properly and such. Treatment of personal data could be thought of as under a contract between government and citizens. For user consent in data release, government could offer citizens choices, with one offering indicating: 'Anything you tell us, we will share,' and another indicating, 'Anything you tell us, we will keep private.' Government could then see which one people preferred.

A real-life example of an individual interacting with different government agencies showed how 'the policy objectives of *integrated* delivery, *integrated* planning and processes and *integrated* governance may sound laudable and attractive' – but a real person often needed 'real and dependable boundaries around her relationships, and separation of the information.' It should not be assumed that more was always better in integration. If a person were to trust agencies with personal data, that individual had to have a seat at the table. Identity management and data sharing would need to be 'co-constructed by the individuals involved within the context of the individual cases and relationships.'[24]

[24] Mike Martin, 'Representing Identity and Relationships in Information Systems,' Position Paper for the forum on e-Infrastructures for Identity Management and Data Sharing.

Local government could serve as an agent of the citizen. With respect to governments' serving a democratic function, a citizen could have a 'personal information broker,' with this service provided by local government. The local government would serve as an identity provider guarding a person's identity information, and the user could log in, controlling information release in a user-centric approach. This model could help accommodate the digital divide by simplifying processes for people and providing access to the infrastructure.

Microsoft's experience with Passport had taught a valuable lesson: It showed that users did not want one large entity to be at the centre of all their data and relationships and everyone else's as well. The wisdom that Microsoft was now spreading was that successful identity systems would be marked by certain characteristics, as described in the box below:

Seven characteristics of highly successful identity systems:[25]

1. *User Control and Consent*: the user controls which information is revealed to another party

2. *Limited Disclosure for Limited Use*: systems don't disclose more information than is necessary in a given context

3. *The Law of Fewest Parties*: systems disclose identity data only to those with a necessary and justifiable place in the relationship

4. *Directed Identity*: supports both broadcast identifiers for public entities and 'unidirectional' identifiers for private ones

5. *Pluralism of Operators and Technologies*: works across multiple technologies run by different identity providers, including government

6. *Human Integration*: works with and is usable by real people

7. *Consistent Experience across Contexts*: behaves the same way wherever and however you use it

Since it was generally agreed that a person had a natural role in managing certain data pertaining to them, the three technical models could be used in combination according to different needs. In addition to promising a more flexible identity infrastructure, the early use of different models simultaneously could help drive adoption and allow a more diverse array of policy choices in the future. There was a continuum of possibilities affording a mix of models according to desired functions.

According to current practice, however, the user often did not have much choice. There were often times when the state would essentially say, 'Sorry, this is for the state's benefit.' If a goal of information sharing was to augment government powers, this fact should be stated explicitly. It would be counterproductive to dress up policy choices in an attempt to make them appear geared toward the citizen's benefit if in fact they were not. Whatever the choice of models along the continuum and the effects on personal autonomy, it was important for government to be straightforward.

At the same time, it would be foolish to base the choice of technology on how citizens wished to interact with government, for predicting technological developments was always risky. (An example here was search engine technology, which confounded

[25] This material is referred to as 'The Seven Laws of Identity' and was developed by Kim Cameron of Microsoft. The characteristics were among points made in Jerry Fishenden's 'Identity Issues and Developments,' Position Paper for the forum on e-Infrastructures for Identity Management and Data Sharing.

many who had poured resources into portals as they tried to anticipate how users would want to access information.) Bottom-up innovation occurred naturally, and it typically defied prediction. Instead of trying to predict technological developments, the focus should be on the organization, even as the objective was to serve the citizen. Recent history provided lessons here as well: For the private sector, the use of new media had of course reconfigured the relationship between business and the individual; but the real benefits had manifest within the firm, where there had been a reconfiguring of who did what job, and where. The major commercial advantages entailed this internal reconfiguring, not the changing relationships between business and consumers. Joined-Up Government assumed there was going to be this sort of reconfiguring.

Again, technologies would be changing rapidly, and it was impossible to predict which ones individuals would embrace for their own purposes, and how they would wish to use the tools. Decision-makers should avoid trying to restrict people.[26]

Meanwhile, time was ticking for the mandated deadlines, and to many it seemed unlikely that the public would come to understand options in time to convey desires to officials whose job it was to meet deadlines.

9. Public Attitudes and Trust

In terms of actual adoption, unless policymakers wished to foist identity management systems onto the public, they needed to ensure that citizens would feel comfortable using the infrastructure once it was operational. There was no point in the government's spending a great deal on developing and advertising new services if citizens would reject them.

People usually opted for convenience when given the choice, and they wanted things to go smoothly when accessing services. To be user friendly, a system should look good on the outside (the 'front end') and cover over-complex relationships that lay behind that facade (the 'back end'). Much work had already gone into the front end, trying to deliver an integrated, seamless experience for the public. In institutional terms, the back end involved a tangled mix of agencies at the local and central levels.

Politically, in explaining and selling the rationale for the infrastructure, it could prove helpful to latch onto a story to tell what was happening on the ground and to describe how changes could be made. Then the technology could be put forward by a politician, taking the role almost of an actor, who would explain it in terms of scenarios, presenting it as a bottom-up approach.

Joined-Up Government aimed to treat people as citizens, with services as a whole attending to the individual. A citizen had many roles, including those of a voter, a tax-payer, etc. Even as government aimed to serve the citizen in these various capacities, the message should be that the citizen was more than the sum of the citizen's roles and the services geared toward them.

[26] David Harrison, 'The Management of Identity & Personal Information on the Internet,' Position Paper for the forum on e-Infrastructures for Identity Management and Data Sharing.

Still, for the public, what did identity management mean? Public perception would prove very important. Besides feeling comfortable with the technology itself, there was also the need for the public to have trust in government as it operated identity systems. How would this trust be garnered?

Accountability to citizens should be a primary concern since an important aspect of citizenship was a person's ability to scrutinize what government was doing. Thus, the public should be able to measure how the system was operating, and the technical system needed to bring with it a sort of signalling for people. To make accountability understandable to the citizen, designers should set flags to tell citizens what choices were being made in the delivery of services and in the treatment of personal data.

Data treatment that differed from what the user expected would raise questions of fair information practices and data protection. New possibilities for information sharing could lead to new uses of personal data – involving a sort of retro-engineering of the original purpose for which data had been captured (in a legal sense) as data was subject to secondary, or downstream, uses. So, too, with the easy transfer of information enabled by identity systems, service providers might demand identity information that they did not actually need. Government would also be accessing personal data for purposes beyond the provision of traditional services associated with that data.[27] Both government agencies and private actors needed guidance on informed consent and other legal requirements for data protection. On a systemic level, it would be important for the identity infrastructure to support best practices in data protection.

The public cared about privacy. In the past people had clicked through privacy statements not because they were indifferent, but rather because they did not feel they enjoyed a true choice: they either had to accept what was written or not engage in a transaction. Research by the Information Commissioner's Office showed that people were beginning to care.

A number of participants viewed data protection tools as an inevitable part of the roadmap for an identity infrastructure; others were sceptical as to whether law could be captured and accurately reflected technologically.

Technology was advancing to enable more effective notice and consent for the user, as called for by data protection law. Some work had been done on 'sticky' policies that could travel with the data. For a user-friendly system to enable people easily to specify preferences for the treatment of their data, there could be a sort of dashboard, where each user would set their own preferences and be able to update them from time to time. The dashboard could be used for both governmental and private sector activities.

Other technologies could work with a system that would enable a person to designate preferences for data protection. By way of example, whereas the financial sector used to have very long terms and conditions with notices buried in the middle, now tools enabled the flagging of concerns up front via a simple message, with further detail then accessible.

[27] It was noted that consent was not an absolute requirement in all cases. Moreover, surveys showed that people did not object to surveillance if it was carried out in the name of catching bad actors, for example those suspected of being terrorists. However, people did mind surveillance if it was directed at their own actions, for example speeding while driving.

Of course, such designs would need to factor in what it was that was causing the public to be mistrustful. Recent findings in the series of Oxford Internet Surveys (OxIS) indicated that 84 per cent of respondents believed that 'personal information is being kept somewhere without me knowing it,' with this figure up dramatically from 66 per cent in 2005.[28] There were cultural differences in trust levels as well, for example between Great Britain and the United States or Singapore. The recent Trustguide[29] study showed that people thought in terms of risk rather than trust. If there were more information available on what was going to be done with personal data and for what purpose, it decreased the sense of risk in that people had definitive information on what would happen. Mistrust stemmed from a sense that people had lost control.

An important element in restoring a sense of control, and a natural component to any system offering redress or restitution, was the ability to audit how data had been treated. One reason an audit trail was needed was that concentration could result among entities providing identity management services. Concentration could bring collusion and other corrupt practices, so audits were needed to prevent this abuse.

As summed up by Bramhall:

> 'Attainment of the Government's vision regarding digital services[30] is threatened by many individuals' concerns over the increased potential for surveillance, over them and their actions, that consuming such services would offer. Adoption of digital service delivery infrastructures whose designs avoid the need to know the absolute identity of the service consumer would significantly reduce that potential and the concerns it creates. The technologies that are needed in such designs exist today and are available for use. However, their widespread deployment and use are hampered by ignorance of their existence and potential, concerns over their business risk and a habit-driven preference for traditional IdM systems. Clear support by the Government for new approaches to system design would provide the necessary catalyst to widen their deployment...'[31]

[28] Bill Dutton, 'Attitudes Toward Privacy and Identity in Britain: 2007,' Position Paper for the forum on e-Infrastructures for Identity Management and Data Sharing. Whereas people who spent a good deal of time online tended to be more trusting in that environment than those who did not, the figure for these users' believing that personal information was kept somewhere without their knowledge was still at 83 per cent (as compared to 88 per cent in the group that did not spend significant time online).

[29] Available at: http://www.trustguide.org.uk/publications.htm

[30] 'Creating a country at ease in the digital world, where all have the confidence to access the new and innovative services that are emerging, whether delivered by computer, mobile phone, digital television or any other device, and where we can do so in a safe environment,' Connecting the UK: the Digital Strategy, Cabinet Office, Prime Minister's Strategy Unit, joint report with the Department of Trade and Industry, March 2005.

[31] Pete Bramhall, Position Paper for the forum on e-Infrastructures for Identity Management and Data Sharing.

10. The Public-Private Partnership in Covering Costs

The notion of support by government raised the obvious question of who would finance efforts to build the identity infrastructure. The group surveyed several countries' recent experiences with national identity cards, and the role of a public-private partnership in covering costs came to the fore.

In Canada, central government agencies did not want to deal with the registration process, so one service was designated to handle registration for all government services; the theory was that the same service could be used for private purposes as well. However, the provincial and local governments did not wish to use this system. The debate had become so heated that policymakers dropped the plan.

The cases of Switzerland and Norway showed that if the public sector financed the infrastructure, the private sector would participate.

Business orientations were different from those of government. Businesses had marketing departments, looking at what the demands and needs were. Understanding the responses to those needs would give a business a niche. Whereas businesses tried to attract customers, the state was different: Agencies were 'puts'. But government still needed both to understand the segments of its customer base and to market to them. In terms of motivations, a commercial company had a clear goal in using identity management services – i.e. profit. What was government's primary objective in using this technology? What were the different requirements in serving customers versus serving citizens?

The UK's initial ambitions for a national identity scheme had proved costly as envisioned systems were inflexible and not tailored to agency needs; as a result, the systems were never deployed. Budget constraints meant that systems which promised efficiencies and cost savings would now receive favour. The Crosby report[32] would spell out a new strategy for the UK identity program and would advocate private sector involvement. Government needed to provide sufficient economic incentive for the private sector to participate.

One view held that there was a clear business case for information brokers in user-centric systems, and that this model would move forward if the public sector would be willing to accept it. The boundaries could be redrawn, and there could be new entities handling the provision of services – at different levels of government (e.g., a local authority delivering a DWP service), or via the private sector (e.g., a company providing access to a government service and meanwhile offering the citizen other services). Businesses could help governments in exchange for access to customers. (For example, Microsoft and Google had offered free email to higher education institutions, and the only thing they received was a long-term relationship with the students.)[33] For an infrastructure to accommodate different models simultaneously, it

[32] http://www.hm-treasury.gov.uk/independent_reviews/identity_management/identity_management_index.cfm (Official publication forthcoming).

[33] Of course, public and private actors had different responsibilities, for example with respect to confidentiality.

made sense to consider if there were the parts of the economy where the user-centric approach was the logical one and where there would be a critical mass for uptake; these services could then converge with the organization-centric approach in a few years' time.

Another view held that instead it was the other way around: If government would specify the requirements, private sector developers would come forward to build appropriate technologies. Government should set out a framework that would allow components to evolve. The market would then produce the specific architecture. While accommodating legacy databases would be relatively trivial cost-wise, it might not make sense for this objective to dictate technology choices for the future. Government should avoid imposing a technology, especially one from the 1980s.

There was a need for technology designs to be flexible for the long-term since public policy would change. Data sharing in a non-electronic environment provided an apt analogy as policies for privacy had always been evolving; likewise, technology should not hard-wire in properties that might later interfere with any possible policy setting. Policymakers would do well to discuss with technologists longer-term organizational aims and flexibility needs. The technologists could then design a framework that could adapt over time and avoid large redesign costs that could otherwise come with policy reversals.

Rather than thinking in terms of what should be implemented in what phases for the roll-out of a 'master plan', it was important for decision-makers and designers to think along the lines of being able to transition architectures for policy requirements, as they might later be adapted.

Local authorities were perhaps more inclined than central government to see how user-centricity was a business concept as it drove value. Could local authorities actually deliver real value to the citizen, or was it the private sector that did this well? Local authorities recognized that it was not their job to build infrastructure, but that they did have a role in seeing that the infrastructure provided value to the citizen.

It was suggested that the best way to build a citizen-centric system would be to 'park' current systems and start afresh. Policymakers had not yet given serious attention to the long-term advantages of doing so. Such a transition could take some time – even 15 or 20 years – but this move would allow (an arguably necessary) complete overhaul.

Network effects would prove important – that is, the value of the network would increase with the number of nodes. In this respect, long-term vision was needed for investment. Decision-makers should also think about how an identity infrastructure could help generate economic activity and create tax revenue to help cover costs.

As a general matter, it was noted that no figures had been estimated for the cost of *not* adopting identity management technologies.

Still more broadly, it was questioned whether the implicit assumptions about what constituted costs and benefits were right, in the light of the public interest.

11. Pilot Project in the Education Sector

The group then considered whether a particular sector offered promise for a pilot project so as to allow an identity infrastructure to take root and gain public acceptance. Education, health, financial services, and immigration were all candidates.

The education sector stood out as a suitable sector for a pilot project for a number of reasons. It made sense to start with a population likely to find the technology easy to use, and education involved young people who were highly computer literate. In addition, students' relatively rapid movement from one institution to another (e.g., primary to secondary to tertiary levels) would allow testing of information sharing across institutions. Experiments could be tweaked as new crops of subjects would be available every few years for test-case purposes.

Education could be viewed as a 'friendly' pilot project since data here was of a happy nature, pointing to people's positive accomplishments (i.e. what they had learned and hurdles they had overcome). Even if an identity system in the education sector were also intended to convey 'unhappy' data (such as concerns from the police, social workers and teachers about the potential of young persons to become productive adults)[34], the general population might view the pilot identity system as bringing individuals convenience and efficiency as they set out to achieve more.

In addition, by involving children's data, the sector would provide practice in observing particular data protection requirements.

Education also combined both public and private sector dynamics. It entailed a competitive market, but this market was less chaotic than the purely commercial market, and the government could require common approaches among different institutions in the sector.

Because education involved life-long learning, this pilot project would support the government agenda of instituting an identity management system that would follow a person throughout their life.

Finally, education would serve as a test-case for jurisdictional issues. It involved different levels of government as it required links between central and local authorities. In addition, it could test dynamics of international integration in identity management. The Bologna Process within the European Union was lining up an identity management system, with proof of concepts already in place. The difficulty was not at the technical level, but rather at the political level, and education could help show how these political challenges could be overcome.

[34] Anderson, R., Brown, I., Clayton, R., Dowty, T., Korff, D., Munro, E. (2006), 'Children's Databases – Safety and Privacy,' Information Commissioner's Office. Available online at: http://eprints.ucl.ac.uk/archive/00003878/01/3878.pdf

Several specific initiatives could tie into a pilot project:

JISC currently had underway its Identity Project and its e-Infrastructure Security Levels of Assurance (ES-LoA) project.[35] The Identity Project would 'research into and establish consensus in the current practice and future needs of UK academic institutions in identity management.'[36] Meanwhile, the ES-LoA Project would 'examine existing definitions of authentication levels of assurance, both at UK and international levels, building consensus and making proposals regarding standard definitions for use in the UK education and research community.'[37]

There were several potential collaborative development projects among the IT departments of five regional universities (Newcastle, Northumbria, Durham, Sunderland and Teesside) and other partners. The projects included one called EPICS-2, which would extend the largely illustrative case studies of previous collaborative work to 'large-scale cohorts of real learners' data' and capture 'much needed evaluation data on student and staff perceptions of the value of transferring data;' that project would also 'provide extensive pilots and well evaluated case studies in using ePortfolios to support personalized learning.' Another proposal submitted, called Shared Services, ePortfolios and the Management of Identity, 'would take multiple actors from multiple institutions' (e.g., secondary schools, higher and further education institutions, and local authorities), and map out processes and the necessary business requirements and specifications 'to enable a learner to move from one institution to another.'[38]

The DCSF, meanwhile, 'was aiming to develop a coherent approach to recording and verifying the details of children, learners and the school workforce.' The effort would give the Department the chance to align its approach with the cross-governmental identity management work. Exploratory work 'to develop a full business case, including risks, costs, benefits and savings' would proceed, with a view to recommending the way forward. The exploration would facilitate work on a 'detailed architecture' and 'implementation plan' to:

- Link appropriate DCSF and third party systems.
- Develop a unique, public facing education identifier.
- Allow other DCSF systems to join a federated system, as and when necessary.[39]

[35] Matthew Dovey, Position Paper on ID and Personal Information Management on the Internet, produced for the forum on e-Infrastructures for Identity Management and Data Sharing.
[36] Id. For additional information, see: http://www.angel.ac.uk/identity-project/index.html
[37] Id. For additional information, see: http://www.es-loa.org/
[38] Paul Hopkins, Position Paper for the forum on e-Infrastructures for Identity Management and Data Sharing.
[39] Keith Holder and Darren Egan, 'DfES Identity Management (IDM) Background,' Position Paper for the forum on e-Infrastructures for Identity Management and Data Sharing.

12. Conclusion

Key themes throughout the forum included the desire to promote efficiency and convenience in public services; the need to prevent function creep in government use of data; the role of data protection laws and technological designs in ensuring sound systems; the importance of choosing technologies according to long-term goals; agency pressure to act quickly in light of looming deadlines; and the hint of a global identity infrastructure. It was clear that more dialogue was needed on these topics.

Because plans for a national identity card were moving forward, this dialogue had to happen quickly. This urgency in mind, the Department of Business, Enterprise, and Regulatory Reform was working with the Identity and Passport Service, the Engineering and Physical Sciences Research Council (EPSRC), and the Economic and Social Research Council (ESRC) to back a three-year research and development programme. This programme would combine social science and technological innovation. Work should seek to balance public expectations of privacy and consent with the potentially intrusive workings of identity services and network security. Research would be cross-disciplinary, with sponsorship funds of £9-10 million allocated for work.

The OII would be glad to organize additional forums in the future. In particular, the Institute would be eager to bring in additional viewpoints to inform work of the public sector.