

Balancing the flavours of data-sharing.



Data-sharing offers greater convenience for the individual, and improved efficiencies for organisations. But it comes in two flavours, 'traditional' back-office data-sharing and an emerging front-office approach. By striking the right balance between them, the public sector can empower individuals, mitigate concerns about privacy, and help overcome the market's failure to meet the need for secure on-line authentication.

'Traditional' data-sharing takes place between organisational back-offices, and requires that the participating organisations create an index to match-up an individual's records across their various databases. The financial sector has been doing this for years to create credit records; the public sector is only now beginning to catch up.

But there is now a new approach that we call front-office or citizen-mediated data-sharing. The principle is very simple: one organisation gives to an individual access to a tamper-proof record of certain personal information, and the individual can then show the record to other organisations when required for the purposes of a transaction. Current paper-based examples include medical prescriptions, exam certificates, and the driving licence.

Replicating this front-office approach electronically requires a new kind of infrastructure, in which an individual commissions an information-broker to intermediate in his relationships with multiple organisations. The broker enables the individual to sign-on securely to these organisations, and to give explicit transaction-based permissions for the sharing of data between them. Brokers may provide authentication in-house, or may outsource this service to specialist authentication providers; banks and mobile operators are well positioned for this role. In time the banks and mobile operators may also act as brokers in their own right, competing with web-centric organisations and others, possibly from the public sector.

Once established, brokers have the potential to deliver a wide range of services. Quick wins include secure messaging, as well as secure single-sign-on. Later we may see person-centric record aggregation, single-point-change-of-contact details, intelligent mail redirection, permissioned marketing, and more.

We argue strongly that the public sector in the UK should pause before committing entirely to back-office data-sharing. In a mature e-economy, there will be a need for balance between the two approaches, as the following points demonstrate:

- **Privacy/control.** Depending on the application, back-office data-sharing may or may not require the individual's consent. If consent is required, the individual is likely to be asked to agree to all 'necessary' data-sharing at the outset of a relationship with an organisation. Such a broad-brush approach may make the individual feel that he is no longer in control of his own information, and that his privacy has been compromised. In contrast, front-office data-sharing gives the individual fine-grained control over every transaction, and is privacy-enhancing.

- **Scalability.** From an individual's perspective, back-office data-sharing tends to blur the boundaries between organisations, and may create the impression that he or she has but a single relationship with the entire group. Thus the back-office approach can only be used by organisations that are closely linked, and it cannot be scaled into a general multi-application solution for use across the economy.

- **Identification vs authentication.** Back-office data-sharing requires that organisations match their database records without any help from the individual. This process can be made much easier if each record contains, or can be linked to, a common system of identification, such as the UK's proposed national identity card (or other sector-specific identifiers). Concerns about top-down state control, and the loss of privacy, are well known. In contrast, front-office data-sharing invites the individual to use a common system of secure authentication to demonstrate ownership of database records, and to create – under his own control – links between them. Privacy is maintained because each organisation uses a relationship-specific identifier for the individual (akin to a customer reference number); common identifiers can be transmitted if required for a particular transaction, and with the consent of the individual.

We come now to the question of which form of data-sharing should be used in which part of the economy. The answer depends on boundaries and relationships.

Central government comprises a small number of departments, each of which is the sole national provider of certain functionality, and maintains one or more databases of personal information. The main examples are the Home Office (Passport, ID Card, Criminal Records), Department of Work and Pensions (NINO), Department for Transport (DVLA), and HM Revenue & Customs.

Most people have no choice but to be recorded on many, if not all, of these databases. They are aware that the departments share data in limited ways, and seem content to trust that internal controls will protect their privacy. Further, as the departments share more data, individuals begin to think that, rather than having distinct relationships with each department, they have a single relationship with central government, and that the departments are simply different facets of the monolith. What annoys them is the evident inefficiency of inter-departmental data sharing, as evidenced by the need to submit the same information – such as change of address – many times over. The faster back-office data sharing can be improved to overcome these problems, the better.

The right approach for other parts of the public sector, outside central government, varies. Starting with education, few people consider that they have a direct relationship with the Department for Education & Skills. Rather, they have relationships with the various schools and colleges which contributed to their education. They would be alarmed if a change of address sent to one learning provider was immediately known by all the others; and – similarly – many believe that only the individual has the right to aggregate records from different learning providers to create a lifelong-learning learning record, also known as a validated CV or (part of) an e-portfolio.

Health is similar to education in that providers exist on both sides of the public-private boundary. However, in contrast to the state education system, the National Health Service is strongly branded and still centrally managed.

Thus people may well consider that their relationship is with the NHS as a whole, rather than with any constituent part, and it is not unreasonable for the NHS to use back-office data-sharing to create aggregate records. That said, there has been considerable resistance to the Connecting for Health proposal to create a national core spine of health data, to the extent that the plans have been successively down-graded from compulsory to opt-out, to opt-in, and then to regional in lieu of national. What people did not like is the notion that records of care received from, say, a hospital in Penzance could be viewed by a medic at the other end of the country, constrained only by ethics and contract. This problem does not arise in an approach based on front-office data-sharing, provided always that the boundaries of a 'single' healthcare provider are drawn sufficiently tightly.

The final major part of the public sector, local government, provides a wide range of services, and a full analysis is beyond the scope of this note. However, for some services, such as the administration of housing benefit, a local authority acts as a direct agent of central government, and here back-office data-sharing with the DWP is clearly appropriate. But for other services, such as the provision of libraries and leisure centres, a local authority is simply one of many potential providers and a front-office approach to data-sharing is indicated.

In summary, then, there would seem to be a strong case for citizen-mediated data-sharing in education, and perhaps in other sectors as well. Given that commercial organisations tend to be jealous of their customer relationships, and thus suspicious of any attempt at intermediation, information brokers are unlikely to reach critical mass if working only in the private sector. This can be regarded as a market failure, since there is little doubt that their services would be valued by consumers. There is thus an opportunity for the public sector to seed the market with one or two lead applications, and also drive standards for interoperability

This note is a brief introduction to citizen-mediated or front-office data-sharing. Longer discussions can be found in:

- o Submission to the 2006/2007 House of Lord's S&T Committee enquiry into Personal Internet Security, led by Eidentity with support from the academic, educational and business communities; and
- o 'Striking the right balance between integration and federation in the UK public sector ...', a paper commissioned in 2005 by the Office for National Statistics from Eidentity as part of the Citizen Information Project.

Both documents are available from John Harrison of Eidentity Ltd. john.harrison@eidentity.co.uk 07801 231 693.