Resolving the Privacy Paradox: Practical Strategies for Government Identity Management Programs

Moderator: Tammy Kulesa
July 28, 2009


John Reiners: Thank you for having me.

Tammy Kulesa: To help set the stage I am going to start from an excerpt from the executive summary of the paper. “The digital age promises to deliver effective identity management solutions for government as citizens demand greater security in their travel and transactions, yet at the same time there is strong opposition on privacy and civil liberties grounds to some proposed government initiatives.

This tension between the power of technology to both empower and control citizens is what we call the Privacy Paradox. We believe it's time for governments to recognize this paradox and like their counterparts in the private sector begin responding to the public demand for identity management solutions that are both effective and engendered trust and confidence that personal data is not being abused.”

John, this is a very powerful statement that I bet prompts many provoking conversations, discussions and ultimately arguments. Could you take a moment and explain what an identity management program is? And what are the types of identity management programs that governments are implementing?

John Reiners: Tammy of course, well identity management is where a process needs to check on an individual's identity before progressing. The effectiveness of the process will depend highly on the quality of information assurance. That is, being absolutely certain that the person is who they say they are to avoid errors or fraud.

So traditional identity management programs are things like passports and driver's licenses and perhaps national identity cards. But identity management is becoming an increasing part of other government programs where personal records are kept and the citizen requires access to government services.

So we can think of things like personal health or social security records. There are of course lots of examples of identity management in the private sector. For example, smart cards to get access to buildings, customer loyalty memberships schemes which collect
personal data on purchases and bank credit and payment cards which check on an individual's identity before authorizing payment.

The digitization of personal records and the growth of powerful new technologies to share and reuse escalating volumes of data has created both fantastic opportunities for government identity management programs as well as some concerns among citizens relating to privacy. This is the challenge referred to in the quote "the privacy paradox" which governments need to tackle.

Tammy Kulesa: Your paper discusses and I quote, "Privacy as fundamental to the issue of public trust which is needed before governments can move forward with their identity management program." Could you elaborate?

John Reiners: Yes, in 2007 the Institute for Business Values surveyed government officials around the world with responsibility for identity management programs. And they told us that privacy was their number 1 and indeed their number 2 barriers to making progress with their programs.

Since then, the issue has become even more pervasive. Every other day one comes across a story in the media relating to concerns about government use or loss of personal data. We think they need to break it down and there are in fact a number of related issues, there is privacy, but also security and data integrity.

Privacy concerns related personal data being misused, security concerns are about improper access or loss of government data and data integrity is about getting data wrong. Citizens have concerns in all three of these areas. And governments need to tackle all of these concerns if they are to convince citizens that new approaches to identity management are a good thing.

The paper focuses on privacy rather than the other two issues. The reason is that it is a particularly complex issue where governments need to convince the public that their programs properly handle personal data at all stages, from collections through to how the data is managed, processed, shared and deleted in government systems.

As government agencies and others are increasingly aiming to join up and share information, including personal information, there are questions about the protections needed on how personal data is used. For example, can a tax authority share personal records with the Social Security department.

Security and data integrity are important issues in their own right. Where I think the solutions lie elsewhere. For example, more secure systems and better management controls to enforce data integrity. If we look further into public attitudes to privacy.

Attitudes will of course evolve as people get more used to sharing personal data. But most studies showed that there are a sizable percentage of people who have concerns relating to privacy. And we would expect that to continue, particularly relating to government identity management schemes.

There is also evidence of a trade-off. People accept some reduction of privacy in exchange for the benefits of the service. This trade-off we explained is a result of the privacy
paradox. How computer systems can both provide fantastic benefits through improved sharing of information, yet also has the potential to control, which raises public concerns.

We argue that governments need to recognize this fundamental paradox and provide solutions which deliver the benefits citizens demand, yet also addresses their genuine concerns relating to how their personal data is used.

**Tammy Kulesa:** In the paper you identified three strategies that have contributed to the success of private programs. And that you believe also practical insights to help governments address both sides of the privacy paradox. Please discuss.

**John Reiners:** Yes, Tammy. We argued there are some excellent examples of successful identity management programs, many of these are in the private sector where lessons can be learned about how to implement successful programs. We have identified three keys recommendations.

Firstly, governments need to design their programs in a way both deliver benefits to all stakeholders and reassures them that privacy concerns are being addressed. In the past, some governments have made the mistake of aiming to sell their programs based on the benefits to government.

For example, increased security and reduced levels of fraudulent access to services. These are important benefits, but may not be sufficient to convince citizens and others, such as private businesses, of the value of the program.

Successful private sector schemes are good at identifying all important stakeholders at the start and ensuring that all have an incentive to participate. We quote the example of Danish Health Care, which is in fact a public sector scheme that successfully dealt with multiple stakeholders, citizens, medical professionals, pharmacies, medical suppliers, health agencies, by involving them all from the start and conscientiously delivering benefits to all groups.

We can think of lots of other schemes, for example store loyalty cards, where customers are incentified to participate. At the same time they need to reassure citizens about privacy by providing assurances about how personal data will be collected and used.

So, they could be clearly define privacy policies, for it's own responsibilities of collecting and managing personal data and rules about when consent is required to make any change to personal data. Policies relating to personal data must be designed with the interest of the citizen in mind. Unlike the plethora of privacy policies currently in use by the private sector, for example on social networking sites.

Secondly, governments need to deploy the latest technologies in ways that deliver improved identity assurance and enhance privacy. There are a number of new technologies available that potentially provide a breakthrough in enhancing privacy.

These so called privacy enhancing technologies, or PETS, include bi-metrics in a number of ways in which data can be anonymized. IBM research is involved in developing many of these. For example the identity mixer, whereby data is anonymized and minimized. So,
you only provide the data required for the transaction, reducing the volume of personal data released.

IBM is also involved in PRIME, which is an EU sponsored project, looking at ways of enhancing privacy in areas such as social networking and participates in the Higgins Consortium, an effort to develop and promote standards which support privacy.

It is also important how these technologies are developed and deployed. An open approach to development using common standards will help reassure the public. Rigorous approaches to software development can be used to demonstrate that privacy is built into the solution.

Government can play an important role in developing identity management standards, which can then be used by others. For example, a recent IBM Parliament Institute study into citizens use of Web 2.0 technologies, shows that many people are concerned about security and privacy, but would prefer as a solution to have confidence in secure authentication rather than for example more restrictive policies for self or independent monitoring of data usage.

This is perhaps an area where a government sponsored identity token can provide that reassurance of digital transactions.

The third strategy is to provide explicit reassurances to the public that if things do go wrong there will be quick and effective remedies. So, they need to have management processes in place to deal swiftly and effectively with any concern about how personal data is managed and used.

Many organizations are designing and implementing policies and procedures for how they deal with personal data. In IBM, for example, there is a chief privacy officer and clearly documented policies for handling of personal data both for employees and clients.

It is also important that there is access to independent advice and redress. That there is some form of policing to ensure that privacy policies are being adhered to. And individuals can appeal to an independent umbers man, if they are dissatisfied.

The report quotes Payment Card International, a consortium of payment card suppliers, who has implemented a data standard and have a system of accreditation of merchants, backed up my independent audit to reassure that they are meeting the standards.

There are interesting developments in this area. Different jurisdictions are developing legal safeguards relating to personal data. For example, the EU’s 95 directive provides stringent obligations on national governments. Whereas in the U.S. privacy legislation and protection has been developed more on an industry level, for example the HIPAA legislation, or state level.

We would expect to see further enhancement of privacy protections and international harmonization as we confront many of the difficult issues about governance of data as it crosses borders, for example with cloud computing.
Tammy Kulesa: In conclusion, what is your suggestion on how private and public organizations should tackle these complex issues?

John Reiners: My conclusion would be above all that identity management can be done and indeed it should be done now. Privacy is a genuine concern to citizens and consumers, which I can only see escalating in significance and potentially acting as significant constraint to progress.

Technologies are available now, which if implemented in the right way can greatly improve confidence in identity assurance. Governments can help to promote high quality standards that could then be adopted by others.

Those considering implementing identity management programs can learn from successes elsewhere and provide the effective solutions that deliver benefits to citizens and consumers while addressing their genuine concerns about privacy.

Tammy Kulesa: John, thank you for taking the time to share your findings on the complex issue of the privacy paradox. To download the paper, please visit ibm.com/gbs/privacyparadox.