INFORMATION
INTEGRITY
SOLUTIONS

The Trust Cluster: Dealing Effectively with *Security, Privacy, Identity* and *Authentication* at the Heart of Connected Government

Malcolm Crompton

Managing Director, Information Integrity Solutions Pty Ltd

Privacy Commissioner of Australia, 1999 – 2004

www.iispartners.com

Stockholm

9 December 2005

Introduction

Whether it is business or government seeking to provide a service or sell a product, individuals will not respond unless they trust the offering. Online options can magnify these issues because it is a new channel that many people still do not understand and because of repeated stories of untrustworthy online public and private sector activity. Convenience or other overwhelming reasons to take up the offering may mask this to a degree, but that is all.

In other words, the 'Trust Cluster' Track is arguably the most important of the discussions that will be held at the Public Services Summit.

This paper sets out to introduce the issues and raise some of the questions and dilemmas currently posed regarding this key enabler.

What is Trust and why is it important?

There are endless writings on this question. Here is an overview.

The National Institute of Governance of the University of Canberra ran an excellent seminar in August 2005 that directly addressed the question.

At the seminar, Professor Geert Bouckaert, Director Public Management Institute, Katholieke Universiteit Leuven (Belgium), quoted the following three definitions:

> Baier: "Trust involves the belief that others will, so far as they can, look after our interests, that they will not take advantage or harm us. Therefore, trust involves personal vulnerability caused by uncertainty about the future behaviour of others, we cannot be sure, but we believe that they will be benign, or at least not malign, and not act accordingly in a way which may possibly put us at risk."
>
> Sztompka; "trust is a bet on the future contingent actions of others"
>
> Gamson: "[Trust is] the probability [...] that the political system (or some part of it) will produce preferred outcomes even if left untended"

In the view of Professor Bouckaert, 'Trust' implies that there is uncertainty, because the other party has a certain amount of freedom in his or her actions. In a situation of certainty, trust is not necessary.

One of the most interesting recent and comprehensive books on trust and its importance in public life is "Trust from Socrates to Spin" by Kieron O'Hara, published by Icon Books in 2004. He asks why trust is a fundamental civic virtue. He considers it is "because it saves so much time". Trustful people don't have to spend their lives suspiciously checking each other out, acquiring lengthy track records of good behaviour, or stripping down both engines before boarding a plane. He also poses the question of why voters tell pollsters that they mistrust politicians, but they still vote for them, using the current Prime Minister of the United Kingdom as a particular example. He also analyses different models of trust in particular kinds of professions and services such as the medical profession.

The head of the Australian Public Service, Peter Shergold, believed he had a partial answer in his presentation to the NIG seminar in August. Drawing on the most recent Federal election

campaign in Australia where 'trust' in the leaders of the two main competing political parties were a key issue, he noted that two meanings were being used, one by each leader:

Honesty (to act truthfully) = motives

vs

Capability (to act effectively) = performance

He argued that the winning bid, as measured by the election outcome, was trust in performance not motive. The incumbent Prime Minister won on a track record of delivery and competence.

Online, untrustworthy behaviour has had a significant impact, especially over the last year. Customer trust levels are falling.

Over 90% of Australians think that organisations are asking for irrelevant information or collecting data for other than the stated purpose and they think this is an invasion of their privacy.[1] Both the Yankelovich and Westin surveys,[2] released in mid 2004, indicate that customers are moving from simply resenting this to taking action, including by taking business elsewhere. In the private sector, this can reduce the impact of a marketing campaign by 20%.[3]

Financial institutions face additional challenges such as:

- Anti Money Laundering law, which regulates when they can trust the customer;[4]
- Perceptions of declining customer service through automated, depersonalising services, made worse with a veneer of unsought personalisation that only irritates

The huge security breaches[5] in the USA over the last year have had a massive impact on consumer confidence and their trust in online services. The latest surveys[6] indicate for example

---

[1] See both the 2004 and 2001 Community Attitudes Towards Privacy surveys commissioned by the Federal Privacy Commissioner of Australia, online at www.privacy.gov.au/business/research/index.html

[2] *The State of Consumer Trust Report*, Yankelovich Partners, www.yankelovich.com, available online at www.compad.com.au/cms/prinfluences/workstation/upFiles/955316.State_of_Consumer_Trust_Report_-_Final_for_Distribution.pdf; and
Consumer Privacy Activism Survey, commissioned by Privacy & American Business, headlines online via www.pandab.org at www.pandab.org/pabsurvey04pr.html

[3] Based on Ponemon's Trust Surveys, as reported by *Computerworld* on 28 December 2004, online at: www.computerworld.com/printthis/2004/0,4814,98448,00.html

[4] The Financial Action Task Force (FATF) 'Forty Recommendations' and the Basel II accord; see: www.fatf-gafi.org/document/28/0,2340,en_32250379_32236930_33658140_1_1_1_1,00.html and www.bis.org/bcbs/index.htm

[5] The Privacy Rights Clearing House has documented over 50 million identities compromised since the Choice Point data breach of February 2005
www.privacyrights.org/ar/ChronDataBreaches.htm

[6] "Consumers Still Don't Trust the Internet", media Connection, 14 November 2005, online at www.imediaconnection.com/global/5728.asp?ref=http://www.imediaconnection.com/content/7275.asp
"Report: ID Theft Haunting Bank Customers", Internet News, 11 November 2005, online at www.internetnews.com/stats/print.php/3563566
"Web Users Increasingly Wary", Media Post Publications, 27 October 2005
http://publications.mediapost.com/index.cfm?fuseaction=Articles.showArticleHomePage&art_aid=35558
"Identity Theft Still Threatens Online Banking", DMNews.com, 21 Oct 2005, online at www.dmnews.com/cgi-bin/artprevbot.cgi?article_id=34497&dest=article
"Internet Marketing, Privacy Survey Finds Relevancy the Key", Dodoma, 3 February 2005, online at: www.dotomi.com/new/newsevents/articles_5.html#article6

that nearly a third of consumers report reduced overall use of the Web and nearly a quarter saying that they no longer make online purchases. Consumers are still saying that they do not want to be tracked online, a result which many surveys have strongly detected over the years and which indicates that this sentiment is unlikely to go away.

Law makers and policy makers are expected to respond, but how they should do so has been very controversial. International cooperation in the fight against Spam[7] is generally considered a step in the right direction but rarely considered sufficient. The recent spate of data losses by data aggregators and banks in the USA has led to the US Congress looking at new legislation to protect personal information, but it is being criticised for taking too little action too late.[8]

Although there is variation between economies, consumers everywhere eventually reach a level of concern where they no longer accept a situation of low security and regular loss of privacy though inappropriate use and sharing of information, even if legal.[9]

There is similar evidence with regard to trust in government and its handling of personal information, especially online.[10] Understanding attitudes on privacy expectations and the provision of government services remains difficult and subtle. For example, a recent survey by the Australian Government Information Office concluded that "Privacy issues have been an area of intense focus in e-government planning. Governments have approached this area sensitively to ensure that citizens retain trust in the Internet as a communication channel and for delivery of government services. However, the survey revealed that concerns about personal privacy were a minor barrier to e-government use." On the other hand, when it comes to identity issues, the survey also noted the desire to be able to interact with government anonymously and the steps that individuals took as a result, for example making contact by phone instead of online.[11]

Further developments in technology and government regulation may add to an unsettled community attitude towards government and its handling of personal information about them.[12]

---

[7] See, for example, the FAQ *What is the Australian government doing to stop spam?* It has been issued by the Australian Communications and Media Authority, online at: www.acma.gov.au/ACMAINTER.4784448:STANDARD:1925545571:pc=PC_2913; see also The London Action Plan of the International Forum for Anti-Spam Enforcement Authorities signed by regulators from Australia, the US, UK and many others at www.londonactionplan.com

[8] See, for example, "Data leaks stunt e-commerce, survey suggests", MSNBC, 15 June 2005 online at: www.msnbc.msn.com/id/8219161

[9] One of the best cross-economy consumer surveys on privacy is "Attitudes and Behaviours of Online Consumers: A Study of five Cities", presented by M. Rivera Sanchez (National University of Singapore) to the 26th International Conference on Privacy and Personal Data Protection, 14-16 September 2004, Wroclaw, Poland, online at http://26konferencja.giodo.gov.pl/data/resources/RiveraSanchez_pres.pdf

[10] See the trust in government questions in both the 2004 and 2001 Community Attitudes Towards Privacy surveys commissioned by the Federal Privacy Commissioner of Australia, online at www.privacy.gov.au/business/research/index.html;
"The New e-Government Equation: Ease, Engagement, Privacy and Protection", Hart-Teeter Research in US, April 2003, online at:
www.excelgov.org/usermedia/images/uploads/PDFs/egovpoll2003.pdf
"Privacy and data-sharing: The way forward for public services", UK Cabinet Office, April 2002, online at: www.strategy.gov.uk/downloads/su/privacy/index.htm; the underlying survey work being especially interesting and online at www.strategy.gov.uk/downloads/su/privacy/papers/perri6.pdf

[11] "Australians' use of and satisfaction with e Government services", Australian Government Management Information Office, 20 June 2005, online at:
www.agimo.gov.au/publications/2005/june/e-government_services

[12] "Data Protection: the next 21 years? The operating environment", presented by Malcolm Crompton to a seminar hosted by the Information Commissioner, UK on 29 November 2005 but yet to be posted online; for a similar paper, see "The Networked Society: Identity, Surveillance and Privacy", prepared

What is the Trust Cluster?

Security, Privacy and Identity, or more particularly Identity Management, appear to be the core of the trust cluster.

Security can be hard to define, especially because it is most often perceived by its absence. At its simplest, security "is being free from danger". As noted by the Wikipedia, "Security is a vast topic including security of countries against terrorist attack, security of computers against hackers, home security against burglars and other intruders, financial security against economic collapse and many other related situations". As a technical term, "security" means that something not only is secure but that it has been secured. Put differently, Wikipedia observes that "a secure system is a system which does exactly what we want it to do and nothing that we don't want it to do even when someone else tries to make it behave differently".

It is very often true that people's perception of security is not directly related to the actual security. For example, a fear of flying is much more common than a fear of driving; however, driving is generally a much more dangerous form of transport.[13]

Privacy is another concept given many meanings and definitions. In 1890, in what is now regarded as the first key modern writing on privacy, Samuel Warren and Louis Brandeis popularised Judge Cooley's suggestion that privacy is the 'right to be let alone'[14] and argued for the need for a legal protection of this right in the face of 'recent inventions and business methods'.

More broadly, privacy has been divided into four separate but related concepts:[15]

- information privacy – involving rules for the handling of personal data;
- bodily privacy – protection of our physical selves against invasive procedures;
- privacy of communications – security and privacy of mail, telephones etc; and
- territorial privacy – setting limits on intrusions into domestic and other environments.

Interestingly, more and more economies are introducing privacy laws with a broad based coverage. Those economies that are not doing so have been the subject of considerable criticism especially if they are providing significant business process outsourcing for other economies. This would not be happening without underlying demand from electors for some action to respect the personal information about them that government is handling.

A number of writers have concluded that Identity and hence Identity Management is the 'glue' that can hold together all of the personal information about an individual. It is arguably THE privacy issue of the moment – got right, it can enhance the lives of the population at large; got wrong it reduces them all to the status of laboratory rats in a huge, global experiment in observation and control.

---

for a Baycorp seminar held on 24 August 2005, online via www.iispartners.com at www.iispartners.com/baycorp.pdf

[13] The Wikipedia definition of security is available online at http://en.wikipedia.org/wiki/Security

[14] Samuel Warren and Louis Brandeis, 1890, 'The Right to Privacy', 4 Harvard Law Review 193, 1890, online at www.louisville.edu/library/law/brandeis/privacy.html. They credit Judge Cooley in his *Torts* (2nd edition, 1888, p. 29) with the phrase 'the right to be let alone'.

[15] "Privacy and Human Rights 2004: An International Survey of Privacy Laws and Developments", Privacy International, London and Electronic Privacy Information Centre, Washington, November 2004, online at www.privacyinternational.org/survey.

For the same reason, organisations either public or private seek information that is connected to an 'identity' because that is often how they add value.

'Identity' is a very subtle concept.[16] Often, it is not necessarily the 'identity' individuals would assign to themselves through their lifetime or in any of the myriad roles they occupy, be it any of parent, employee, dance party goer, student, professional society member, seeker of credit or anything else. Sometimes individuals seek these identities and are likely to be quite happy or even flattered by them. At other times, they are identities with characteristics assigned by a person or organisation that has been gathering and analysing personal information believed to be related to that identity. A credit rating is one example of this, and in these cases the people affected often have only a dim understanding that it is either happening or what it means.

Indeed, it is important to distinguish between an 'Identity' that has been assigned to an individual and the 'profile' developed about that identity using the information linked (rightly or wrongly) to the identity. 'Identity' seeks to define the physical person. That identity then is used to seek links between the various elements of our personal histories that have been recorded in order to build a profile. The history includes behaviours and events in which the physical person has participated.

Moreover, either because of the lack of more subtle thinking or because organisations are actively seeking more information about us, identity is used to authorise or collate activity when it is not inherently necessary, even when the technologies exist to avoid such surveillance.[17]

For the purposes of the discussion here, though, some more precise definitions are needed.

Identity Management can be defined by starting with the concept of the entity that is being identified:

- **Entity** – An organisation or person making statements or claims to be authenticated.
- **Identity** – A particular presentation of an Entity, including a particular role being played by the Entity.
- **Evidence of Identity** – Proof (eg: in the form of documents) used to substantiate the Identity of the presenting party, usually produced at the time of Registration.
- **Registration** or **Enrolment** – Establishment of someone's identity and/or entitlement before issuing them with authentication credentials such as an identity token.
- **Authentication** – The process of testing a statement or claim, in order to establish a level of confidence in the statement's or claim's reliability.

---

[16] This subtlety is explored further in "Proof of ID required? Getting Identity Management Right", by Malcolm Crompton when Privacy Commissioner, March 2004 – in HTML, PDF or Word – online at: www.privacy.gov.au/publications/index.html#S

[17] See, for example:
"Proof of ID required? Getting Identity Management Right"; and
"ID Cards - UK's high tech scheme is high risk", London School of Economics News Release, 27 June 2005 and from there, link to the LSE Report titled "The Identity Project: an assessment of the UK Identity Cards Bill and its implications", online at: www.lse.ac.uk/collections/pressAndInformationOffice/newsAndEvents/archives/2005/IDCard_FinalReport.htm

- **Identity Management** – A set of processes and supporting infrastructure that enable the authentication of identity assertions. Very importantly, it is often based on a two step process:
    1. Enrolment in order to have an Identity on which others are willing to rely; and
    2. Authentication of subsequent assertions of an Identity

Identity Management services are emerging as critical to enabling and coordinating relationships and interaction between individuals and other individuals, organisations and items in the world around them.

Finally, many commentators including Jamie Lewis, CEO and Research Chair of the Burton Group (www.burtongroup.com) consider that Identity Management is to be considered in terms of the social issues being addressed not the technological issues. On that basis, Jamie Lewis considers that the core challenge to be addressed are not 'trust' but more specifically cooperation and reliability.

Approaches to Trust

How to generate trust, or be trustworthy, is a very important part of the debate over trust. Kieron O'Hara in "Trust from Socrates to Spin" points to the contradictory models that suggest that a consistent, one size fits all approach is not even possible.

At the risk of over simplifying, an individual or organisation or system is more likely to be considered trustworthy when it demonstrates many of the following characteristics to the other party:

- Known
- Predictable
- Acts in the other parties interests
- Respectful, in deference to the position of trust
- Shares control where appropriate
- Open and transparent
- Accountable
- Safe, for example accepts responsibility for and addresses failure and error.

As an example, compare this list with the traditional image of the London Bobby and how that police force went about policing their 'beat'.

Jamie Lewis likes the approach taken by Robert Axelrod:[18]

> "The foundation of cooperation is not really trust, but the durability of the relationship.
>
> When the conditions are right, the players can come to cooperate with each other through trial-and-error learning about possibilities for mutual rewards, through imitation of other successful players, or even through a blind process of selection of the more successful strategies with a weeding out of the less successful ones.

[18] "The Evolution of Cooperation" Robert Axelrod, Professor of Political Science and Public Policy, University of Michigan, http://www-ee.stanford.edu/~hellman/Breakthrough/book/chapters/axelrod.html

Whether the players trust each other or not is less important in the long run than whether the conditions are ripe for them to build a stable pattern of cooperation with each other."

The dominant paradigm – one way trust

"Information is power" is an old adage that remains very fresh in the information age. Most governments are implementing programs based on collecting and sharing more information including about individuals, with the UK "Privacy and Data Sharing" project but one example.[19]

As a consequence, access to and use of such information can be a point of contention. The ensuing risk assessment and management by the organisation that has collected and handled the information is likely to be conducted from the perspective of that organisation. This in turn can lead to the organisation seeing itself as inherently trustworthy but needing reason to trust others who want to access and use the information.

A simple example is the everyday "User Name and Password" sign on for accessing networks, bank accounts and many other services and entitlements. Something, for example a computer or a service being accessed through a computer, asks the individual to make an assertion which is then authenticated, in this instance a name and a secret. But rarely does the something offer the same in return.

The one way trust approach suffers from at least three weaknesses.

The first is simply common courtesy. The entity asking for the User Name and Password is basically indicating that it does not trust the other party, but is not recognising that the other party may have no more reason to trust the entity. The move towards stronger authentication, ie beyond simply asking for user name and password, will accentuate this.

The second is that it has created a security weakness that is now being very rapidly exploited. Lack of authentication by the entity to the individual, for example, is a significant component of 'pharming' whereby an individual is tricked into giving away such information as User Name and Password to an impostor.

The third and possibly most fundamental is the asymmetric sharing of control. The issuer and authenticator of an Identity such as a User Name have considerable power. At their whim or for other reasons including simple error, they can block an individual's access to services or facilities that the individual otherwise considers ought to be available. A corresponding asymmetry of risk allocation may be associated with this asymmetry. In other words, the risk of a failure of some sort may be borne entirely by the party least able either to bear the risk or mitigate the risk, namely the individual.

These are likely to be some of the reasons why there seems to be particular sensitivity and lack of trust in strong identity management arrangements when they extend beyond small pools of trust (such as the small pool of trust between a bank and its customers or an employer and its staff). The extremely poor record of the Social Security number in the US has a lot to answer for this. It is probably making the Real ID Act much less acceptable than it otherwise would be

---

[19] "Privacy and data-sharing: The way forward for public services", UK Cabinet Office, April 2002, online at: www.strategy.gov.uk/downloads/su/privacy/index.htm

in its effort to standardise driving licences in the US.[20] The French government recently abandoned plans to introduce a more robust electronic ID card[21], as has the government of Taiwan.[22] The ID card proposals by the UK government have also been dogged by controversy for similar reasons.[23] The media debate in mid 2005 over the possibility of an identity card in Australia would suggest that the issue remains controversial there, too.[24]

The emerging paradigm – mutual trust

A market response to the problems of one way trust is currently emerging. Against the characteristics of trustworthy behaviour, mutual trust would seem to be greatly facilitated by mutual authentication.

In a recent study for an Australian bank,[25] the move by a number of banks towards various forms of mutual authentication was obvious. Bank of America, for example, has begun trialling the Pass Mark program which includes the bank authenticating itself to the consumer by sharing back a shared secret in the form of a mutually agreed image that only both parties know. Another company standing in the market with a similar product is Coat.

Importantly, some of the technologies behind stronger forms of authentication already deliver mutual authentication, but this fact is not obvious to the individual user. There are easy ways of making this obvious that may contribute significantly to mutual trust.

What is Government and why does it matter?

This set of questions has been the subject of discussion for centuries, both before and after Plato wrote The Republic.

For these purposes, though, what matters are the characteristics of government that separates it from any other part of society. In that regard, the most important differentiating characteristic is the coercive power of the state. This requires a high level of trust by the citizens of the state or a great deal of unchallengeable power (or combinations). Regardless, the most fundamental use of this power is to control the borders of the state then within the borders, use the power to provide law, order and to raise taxes. The taxes in turn can be used to purchase or supply services to the citizens including more indirectly impact on markets.

---

[20] See for example "New plans are in store for an old number", The Christian Science Monitor, www.csmonitor.com, 10 August 2005, online at www.csmonitor.com/2005/0810/p12s03-ussc.html

[21] "Launch of French e-ID card could be postponed", government News, 20 July 2005, online at: www.europa.eu.int/idabc/en/document/4476/194

[22] "Taiwan Constitutional Court places fingerprinting plan on hold", Privacy International, 22 June 2005, online at: www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-249615

[23] "ID Cards – UK's high tech scheme is high risk", London School of Economics News Release, 27 June 2005, online at: www.lse.ac.uk/collections/pressAndInformationOffice/newsAndEvents/archives/2005/IDCard_FinalReport.htm
On a lighter note, see "the very model of a modern labour minister : a tribute to charles clarke and his id cards", eclectech, at: http://eclectech.co.uk/clarkeidcards.php.

[24] See for example "Identity card not part of war on terror", Editorial, *The Courier Mail*, 19 July 2005, online at: www.couriermail.news.com.au/common/story_page/0,5936,15971974%255E13360,00.html

[25] "Report on Strong Authentication Initiatives By Banks In North America and Europe", completed by Glenbrook Partners LLC and Information Integrity Solutions Pty Ltd for Westpac Banking Corporation, October 2005; copy available for sale through Malcolm Crompton

The rapid creation of the networked society has the potential to impact very significantly on what government can and cannot do. This is because it challenges the fundamental foundation of this construct, especially the ability to control the borders. Information (including financial information and hence finance) is now able to move across borders more easily and uncontrolled than previously.

In a move that preceded the Internet component of the networked society but definitely facilitated by it, government has further blurred the boundaries between itself and other parts of society by outsourcing and selling off services and businesses that were often perceived previously as 'core government'.[26] Government no longer "Builds, Owns, Operates" with the enthusiasm of previous decades. Some of this is the pendulum of policy swinging back and forth. For example, the Royal Navy over which Samuel Pepys had so much influence in the 17th Century was such an outsourced operation that eventually the UK government had to in source a number of components again. Nevertheless, the current approach is likely to be a sufficiently long term trend to see out the careers of many people in the workforce today.

However, government often still wants to shape society. It now relies more on other tools, ranging from purchasing historical services that have been outsourced, purchasing other services or using burgeoning regulatory structures to achieve its aims.[27]

As part of this trend, government is also standing back more often from emerging technologies and services in the economy. A very large component of the information infrastructure that supports the networked society has been constructed in the last decade entirely by the private sector. This has also lead to a different role for government when, for example, the security of the information infrastructure is challenged and needs to be made more secure. Governments are persuading, cajoling, funding change and using other indirect methods for pursuing change but still standing back from "Build, Own, Operate".

This is important because the trustworthiness of the information infrastructure itself can impact on trust in both government and other services provided online.

In addition, increasing levels of cooperation between governments and increasing government use of services provided from overseas means that there is increasing sharing of personal information across borders. This is especially so for financial services, travel, policing, national security, immigration, disaster recovery and major disease and other health matters. There is increasing public awareness of these developments but little evidence of the corresponding translational governance arrangements that might also be expected.

All of these trends impact on 'who do you trust' and 'what do you trust them to do'. In some economies at least, government is seen as inherently more trustworthy than a similar private sector entity. In other economies the exact opposite applies. Blurred boundaries and shifting boundaries reduce predictability and hence for many, also affect trust.

---

[26] The question of what constitutes 'Core Government' was a hot debating point when the Management Advisory Board of the Australian Public Service was writing its report on a decade of reform of the APS in 1993 titled "Building a Better Public Service", MAB/MIAC Report No.12, 1993, AGPS, Canberra

[27] See for example "The Politics of Regulation: Institutions and Regulatory Reforms for the Age of Governance", Jacint Jordana and David Levi-Faur (eds) 2004, Edward Elgar Publishing Ltd

Finally, neither governments nor the people they govern are homogeneous, so it is not surprising that trust in government and its agents vary hugely. In Australia, for example, it is hardly surprising that the Australian Taxation Office has to work harder to be trusted with personal information than other organisations because it is seen to use that information against the interests of the individual. Depending on their vocation, not everybody likes the police no matter how well the policing function is discharged. At the other end of the spectrum, Australia Post is very proud of the extremely positive brand awareness it has generated.

Nevertheless, as a statement of the obvious, the heterogeneity of government also still brings some surprises. For example, the creation of the Department of Human Services in Australia is revealing different levels of trust in its component entities that are still being worked through. For many people who are served by Centrelink, it is difficult to trust. As the major services agency for social security and other benefits payments, it is perceived as seeking personal information to reduce benefit levels. On the other hand, another payments agency in the portfolio, Medicare Australia, is seen in a much more favourable light because it is seen as having much less of an 'enforcement' role. These differences will impact on how and whether the services provided by this Department can be reduced to a single brand.

Security and Privacy

Fundamentally, respecting privacy is simply risk management. The task is very similar to managing security in the company and its products and services.

However, there is one significant difference:

- Security = the company's perspective on risk management of information
- Privacy = the individual's perspective on risk management of information.

Often, these perspectives coincide. For example, neither the bank nor the bank customer want to suffer fraud from Identity Theft, but their point of view may be different about which party should bear what proportions of the risk and the cost.

This issue has been explored many times over the years, including a major paper jointly produced by the Information and Privacy Commissioner of Ontario and Deloitte.[28]

The Information and Privacy Commissioner of Ontario, a leading thinker on the impact of technology on privacy has made the same point in her call for a "Security Technologies Enhancing Privacy" (STEP) program, where she argues that the best security technologies are those that also aim to enhance privacy[29].

---

[28] "The Security-Privacy Paradox: Strategies to address Issues and Misconceptions", Information and Privacy Commissioner of Ontario, 11 August 2003, online at: www.ipc.on.ca/scripts/index_.asp?action=31&N_ID=1&P_ID=14571&U_ID=0

[29] "Security Technologies Enabling Privacy (STEPs): Time for a Paradigm Shift", Information and Privacy Commissioner of Ontario Canada, June 2002; online at: www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=13289&N_ID=1&PT_ID=11351&U_ID=0

Jamie Lewis and Bruce Schneider among others also strongly voice the view that security and privacy should not be treated as opposites or trade offs. Talking particularly of national identity card programs, Schneider states that "I've learned about security over the last 20 years tells me that once it is put in place, a national ID card program will actually make us less secure". While he points out a number of problems with such a program, he states that:

> "… the main problem with any ID system is that it requires the existence of a database. In this case it would have to be an immense database of private and sensitive information on every American – one widely and instantaneously accessible from airline check-in stations, police cars, schools, and so on.
>
> The security risks are enormous. Such a database would be a kludge of existing databases; databases that are incompatible, full of erroneous data, and unreliable. As computer scientists, we do not know how to keep a database of this magnitude secure, whether from outside hackers or the thousands of insiders authorised to access it."[30]

Identity Management

Most traditional identity management designs have essentially required the individual to trust that the organisation with which they are dealing will behave in a secure and honourable way because the underlying technology offers the individual no such assurance and in fact gives the organisation greater power than previously to match and exchange information very cheaply.

Hence the challenge is to discern what good identity management that builds mutual might look like.

Indeed, recent work can now tell us what good identity management looks like. Federated Identity initiatives have made a good start, but more is needed.[31] The work of Kim Cameron at Microsoft with his Laws of Identity,[32] the London School of Economics report[33] and work by the Office of the Privacy Commissioner in Australia[34] have developed very similar approaches. From this thinking, good identity management can be described by the following principles, described in more detail in Appendix A:

- Individuals control the use and disclosure of personal information about them unless specified in law
- Multiple authenticated electronic identities per individual
- Registration empathetic and responsive
- Identity credentials revocable
- Identity numbers invisible outside the identity management system

---

[30] "National ID will make US less secure", Sydney Morning Herald, 19 April 2004, online at: www.smh.com.au/articles/2004/04/19/1082326122398.html

[31] See for example the critique by Stefan Brands, "Liberty Alliance Architecture Analysis", 8 August 2004, online at: www.idcorner.org/wp-content/libertyanalysis.pps

[32] "The Laws of Identity, Kim Cameron, Identity and Access Architect, Microsoft, May 2005, online at: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwebsrv/html/lawsofidentity.asp?_r=1

[33] "ID Cards - UK's high tech scheme is high risk", London School of Economics News Release, 27 June 2005, online at: www.lse.ac.uk/collections/pressAndInformationOffice/newsAndEvents/archives/2005/IDCard_FinalReport.htm

[34] "Proof of ID required? Getting Identity Management Right", by Malcolm Crompton when Privacy Commissioner, March 2004 – in HTML, PDF or Word

- Competition between operators and technologies
- Consistent user experience

Is there a policy sweet spot?

This is where differences in cultures and economies really begin to be drawn out. The question to be answered is what role is there for government in framing solutions for improving trust, especially for online services?

A recent blogging article on the parallels between city architecture and planning and ICT governance rather wistfully notes that "central power must enable interoperability without destroying the benefits that are gained from distributed, loosely coupled services".[35]

However, it may be difficult to find this sweet spot in advance of the actual need for it. This is best illustrated with a couple of examples that show there may be no inherently right answer.

The first example of finding a policy sweet spot is the introduction of digital mobile phones in Europe *vs* North America. In Europe and much of the rest of the world, a specific standard was set up and pricing structures reasonably predictable to users was set up. GSM was the chosen standard in Europe and digital mobile phones were adopted very rapidly. Eriksson and Nokia were almost overnight successes as digital mobile phone manufacturers. By contrast, technical standards and pricing in North America were much less regulated. Digital mobile phone uptake was affected accordingly. For a number of years, individuals could not be sure that their digital mobile phones would connect with each other if they were using different carriers, while pricing structures could make it very expensive even to receive an unsolicited and unwanted call. While it would seem that North America has now resolved these problems, for a while it was a long way behind comparable economies in the uptake of mobile phones. Thus in the case of mobile phones, it seems that strong leadership created better conditions for success.

The second example is the internet itself. It developed so rapidly that there was only a light touch, private sector provided regulatory structure in place to govern its development, for example ICANN and its predecessor, W3C etc. The originators of the internet went to great lengths to argue that the internet should not be regulated or taxed in any way. Arguably the rapid development and the innovation necessary for this to happen could not have occurred if there had been a standards making body keeping a strong hand on developments. As such, the internet is a triumph of uncontrolled innovation and development. On the other hand, we are still living with the consequences, including lower than desirable levels of security and privacy.

Thus in two similar fields of development occurring at almost the same time, opposites of control frameworks appear to have been required for the best results.

In fact, probably the best results derive from the actual tension between the 'planners/standardisers/controllers/you don't have many rights' camp versus the 'let competition rip/libertarian' camp, rather than considering that either camp can get it right to perfection. In other words, the smartest thing to do may be to recognise that this tension is not only a part of the model but an essential part. This is a surprisingly radical thing to say – many would consider that such tensions are imperfections to be eliminated as a 'bad thing' because it

---

[35] "SOA Governance: What We Can Learn from Cities" by Phil Windley, 4 October 2005, online at: www.windley.com/archives/2005/10/soa_governance.shtml

disrupts planning and standardisation (one perspective) or it stops free will, operation of the market place etc (the other perspective). Managing this tension, wittingly or unwittingly, is an extremely difficult challenge for government. Indeed, we should recognise that this summit is simply part of the process.

Very importantly, though, the policy sweet spot may not need strong, regular government involvement if government is able to make market forces to do most of the work. This applies equally to government agencies as it applies to private sector entities.

Two examples suffice to make this point. The first relates to spam, the second to identity theft.

In simple terms, spam continues because it pays. Those who spam will stop when it does not pay. As pointed out by Professor Marshall Van Alstyne of Boston University School of Management,[36] the combined economic impact of effort so far, such as filters, criminal convictions and public education not to open spam etc, have not been enough yet to make it uneconomic. When these and possibly other strategies make spam uneconomic, it will fade away.

Bruce Shneier puts it this way as regards US banks and phishing to commit identity fraud:[37]

> "For years I've written about how economic considerations affect security problems. They can put security countermeasures in place to prevent fraud, detect it quickly and allow victims to clear themselves. But all of that's expensive. And it's not worth it to them.
>
> It's not that financial institutions suffer no losses. Because of something called Regulation E, they already pay most of the direct costs of identity theft. But the costs in time, stress and hassle are entirely borne by the victims. And in one in four cases, the victims have not been able to completely restore their good name.
>
> In economics, this is known as an externality: It's an effect of a business decision that is not borne by the person or organization making the decision. Financial institutions have no incentive to reduce those costs of identity theft because they don't bear them.
>
> Push the responsibility – all of it – for identity theft onto the financial institutions, and phishing will go away. This fraud will go away not because people will suddenly get smart and quit responding to phishing e-mails, because California has new criminal penalties for phishing, or because ISPs will recognize and delete the e-mails. It will go away because the information a criminal can get from a phishing attack won't be enough for him to commit fraud – because the companies won't stand for all those losses.
>
> If there's one general precept of security policy that is universally true, it is that security works best when the entity that is in the best position to mitigate the risk is responsible for that risk. Making financial institutions responsible for losses due to phishing and identity theft is the only way to deal with the problem. And not just the direct financial

---

[36] "The War On Spam Takes A Novel Turn", InformationWeek, 7 May 17, 2005, online at http://informationweek.com/story/showArticle.jhtml?articleID=163104354

[37] "A Real Remedy for Phishers", Wired News, 6 Oct 2005, online at www.wired.com/news/print/0,1294,69076,00.html

losses – they need to make it less painful to resolve identity theft issues, enabling people to truly clear their names and credit histories. Money to reimburse losses is cheap compared with the expense of redesigning their systems, but anything less won't work."

Setting up this environment for government services and powerful identity management systems may be the most important thing that governments do over the next few years to build trust in government online services.

Some important work is under way in Sweden to shed more light on the role of government, business and other interests in building trust in the digital world. It is being undertaken by the International Organisation for Knowledge Economy and Enterprise Development (IKED), which is based in Mälmo. After some years of discussion at various international fora, it is currently finalising work on a scoping study for the establishment of a Global Trust Centre.

However, IKED's initial research is already available as "Enabling Trust in the Digital World, Presentation of a Project on: Exploring Trust and Security Issues, and Examining Opportunities For a 'Clearing House' and 'Global Trust Centre'". This research is available online[38] and is well worth reading for the background research it contains. The final report should be well worth reading.

No magic bullet solution – a framework is needed

Governments appear to be increasingly seeing a role for government in creating trust in the handling of personal information in the wider economy and in their own handling of personal information.

As Privacy Commissioner, I proposed a framework to assist in ensuring that appropriate consideration was given both to the privacy of individuals and other social objectives. The framework – the AAAA framework – also has application in situations where identity management pressures are building.[39]

The essence of the AAAA framework is a life-cycle approach with four elements:

Analysis: Is there a problem? Is the solution proportional to the problem? Is it the least privacy invasive solution to the problem? Is it in line with community expectations? An independent privacy impact assessment will help to undertake this stage adequately.

Authority: Under what circumstances will new powers be exercised, and who will authorise their use?

---

[38] "Enabling Trust in the Digital World, Presentation of a Project on: Exploring Trust and Security Issues, and Examining Opportunities For a 'Clearing House' and 'Global Trust Centre'", International Organisation for Knowledge Economy and Enterprise Development, 2004, online at: www.iked.org/pdf/GlobalTrustCenter.pdf; see also the Global Trust Center website hosted by IKED at www.globaltrustcenter.com

[39] This approach derives from the "AAAA framework" developed by the Office for the purpose of assessing and implementing new law enforcement and national security powers. Earlier versions of this framework were first outlined in an Office paper for the Australian Institute of Criminology's conference in June 2001 (see 'Preserving Privacy in a rapidly changing environment' at www.privacy.gov.au/news/speeches/sp34note.doc) and later in an OFPC submission to the Senate Legal and Constitutional Committee in April 2002 on proposed anti-terrorism legislation (see www.privacy.gov.au/publications/secleg.doc).

Accountability: What are the safeguards? Who is auditing the system? How are complaints handled? Are the reporting mechanisms adequate? And how is the system working?

Appraisal: Are there built in review mechanisms? Has the measure delivered what it promised and at what cost and benefit? Is the measure a permanent or fixed-term solution?

As noted earlier, the number of economies with a privacy law appears to be increasing at a steady pace.

The Asia Pacific region is an example of a region that is still developing its stance on the handling of personal information. Some economies in the Asia Pacific region have had broad based privacy law in place for some years, including Hong Kong,[40] New Zealand,[41] Australia[42] and Canada. Other economies have introduced such laws more recently, with privacy law in Japan commencing on 1 April this year.[43] The United States of America has taken a route that is different again, with many sectoral or specific laws in place.[44] Korea also has sectoral law[45] and is currently debating the introduction of more broadly based privacy law.

In addition, the Asia Pacific Economic Cooperation forum (APEC) has taken active steps to develop and encourage the implementation of the APEC privacy framework.[46]

More specifically, many governments have sought to facilitate improved identity management systems. Examples of better, more privacy respecting approaches include the initiatives in Sweden[47] (generally considered to have the best government initiatives in Europe[48]), Austria[49] and New Zealand.[50] In particular, each of these initiatives allows individuals to choose whether they have an online identity and allow them to have more than one online identity.

---

[40] *The Personal Data Privacy Ordinance*; see www.pco.org.hk

[41] *Privacy Act 1993*; see www.privacy.org.nz/top.html

[42] *Privacy Act 1980* and *Personal Information Protection and Electronic Documents Act 2000*; see www.privcom.gc.ca/index_e.asp

[43] *Personal Information Protection Act*; see www.privacyexchange.org/japan/japanindex.html

[44] These include the *Federal Trade Commission Act*, see www.ftc.gov/ogc/stat1.htm; the Health Insurance Portability and Accountability Act 1996, see www.hhs.gov/ocr/hipaa; the *Fair Credit Reporting Act*, see www.ftc.gov/privacy/privacyinitiatives/credit.html; *The Financial Modernization Act 1999*, also known as the "Gramm-Leach-Bliley Act", see www.ftc.gov/privacy/privacyinitiatives/glbact.html. The Can Spam Act, see www.ftc.gov/bcp/conline/edcams/spam/rules.htm etc

[45] *The Information Infrastructure Protection Act* and *The Act on Promotion of Utilization of Information and Communication Network and Data Protection*; see www.kisa.or.kr/maine.jsp

[46] "Ministers Approve APEC Privacy Framework to Strengthen E-commerce and the Protection of Personal Information", News Release from Asia-Pacific Economic Cooperation, 16 November 2005 with links to the Framework itself, online at www.apec.org/apec/news media/media_releases/161105_kor_minsapproveapecprivacyframewrk.html

[47] Infra Services – a Swedish Way to Facilitate Public E-services Development", ICA Information no. 82 General Issue June 2004 - Article 4, www.ica-it.org/docs/issue82/issue_82_2004_04.html

[48] See www.europa.eu.int/information_society/eeurope/2005/all_about/benchmarking/index_en.htm

[49] The Austrian Citizen Card is described at www.buergerkarte.at/index_en.html

[50] The New Zealand All-of-Government authentication program is online at www.e.govt.nz/services/authentication

One of the better government sponsored research programs into identity management is PRIME, the Privacy and Identity Management for Europe project.[51] Two important privacy enhancing technological initiatives in PRIME are building in multiple identities for each individual and making sure that details of transactions are not unnecessarily recorded. The latter uses a technology called 'trusted pseudonymous transactions' to ensure that a service which authenticates an identity does not also track who is asking for the authentication nor who it is being asked about.

Some suggested steps for government in generating trust in identity and from there, trust in Connected Government

Drawing the strands of this paper together, good practice steps that a government can take or encourage could include:

1. Foster public discussion. Ensure it is open and involves genuine dialogue and engagement
2. Constantly search for and learn from better practice wherever it can be found around the world
3. Use the 4A Framework: Analysis, Authority, Accountability, Appraisal

The end result almost certainly will be a rounded, subtle framework that seeks to respect the individual in an open, efficient society that also respects private life. There will be no 'silver bullet' solution and be wary of anybody who says that there is one. As in all other walks of life, balance is not achieved that way. Instead, trust, identity and Connected Government will be fostered if:

Law + Technology + Market + Transparency + Accountability + Safety = **Privacy & Trust**

Where is this all likely to lead?

The most fundamental issue in the Trust Cluster is control. Individuals mostly want to trust their governments, but not totally.

Identity management systems that depend on one identity per person that must be used in all circumstances will continue to deliver to the identity issuer too much control. Promises made in law will not be sufficient protection against legal but unexpected extensions in the collection, use and disclosure of personal information (so called function creep) and growing illegal uses such as identity fraud.

The minimum consequences of this for identity management in the future are:

- Multiple identities allowed – wherever possible, individuals can choose which identity they use, what information they release and for what purposes
- Identity authenticated only when really necessary – other assertions such as ability to pay or a right of access without identity should always be considered first
- No centralised databases, eg of uses of an identity
- Governance structures that match increased accountability to the increased responsibility that comes with collecting, connecting and collating more and more personal information
- "Internalise the externalities", including full support for helping victims of error

[51] Excellent but lengthy papers on the PRIME project are available on the project's website, www.prime-project.eu.org

The most resilient and innovative solutions will use market forces to achieve these aims to the greatest extent possible, even if law is needed to shape the market to 'internalise' the 'externalities'. The most important will be ways of making sure that government agencies recognise and bear the full cost of any failures, turning them into 'moments of truth'.

The straws are in the wind. Very recent initiatives such as the New Zealand All-of-government Authentication Programme show the desire to build in these kinds of considerations. Even more recently, the Australian Government Information Management Office (AGIMO), has proposed an Australian Government Authentication Framework for Individuals.[52] Released for public consultation only on 5 December 2005, the Framework again has a heavy emphasis on privacy and trust.

Questions and Dilemmas

This paper has illustrated the impact of trust on individual participation, especially in online services. It has offered some thoughts on what is trust and how to generate it and moved on to looking at the components of the 'Trust Cluster' and noted the crucial role played by Identity Management. The paper has reviewed the latest thinking on what might comprise good Identity Management from the individual's perspective then looked at considerations of the role that government might play in creating trust.

This last part of the paper lists some of the questions that might be asked in order to reach specific conclusions in particular circumstances.

- What is the appropriate sharing of control?
  - How do we support this in law?
  - How do we support this by the way we construct new technologies?
  - How do we support this in the way we design Identity Management arrangements?
  - How do we support this in service offerings, eg a "Google on Steroids" Search Engine to find and obtain government services at the time, convenience and frame of mind of the individual or do we build a better portal?

- How do we manage the inevitable failures?
  - Risk assessment
  - Risk allocation as between entities
  - Risk allocation as between an entity and the individual
  - Risk management when the failure occurs, leaving it up to the individual or providing significant assistance?

- What is the role of Government in Identity Management?
  - Provision and authentication of the only trustworthy Identity Credentials for use in all circumstances?
  - Provision and authentication of a 'root identity' to be 'hidden' from everyday use but otherwise the source of trust in any 'derived' Identity Credentials?
  - Other?

- When do we need to authenticate anything?

- When do we need to authenticate identity rather than some other assertion?

---

[52] "Feedback sought on extension of AGAF to individuals", Media Release by the Special Minister of State, Senator the Hon Eric Abetz, 5 December 2005, online at: www.agimo.gov.au/media/2005/december/46809.html

- How can we make Identity Management feel more like a hand shake between equals than a pat down search with rubber gloves on?

- What other role might government play in the Trust Cluster?
  - Security Impact Assessments; Privacy Impact Assessments as routine procedure, at least for major projects

Appendix A

The Essential Laws of Identity[53]

Individuals control the use and disclosure of personal information about them unless specified in law

- Personal information collected for disparate purposes should be kept unlinked and unsinkable
- Any unique identifiers should carry no information about the individual
- Reliance on a central registry of associated data should be minimised
- Use of identifying information by other parties should be limited to the necessary and justifiable in a given identity relationship
- Disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship
- Identity is authenticated only when other assertions are not sufficient and only when necessary

Multiple authenticated electronic identities per individual

- An identity system should allow individuals to create secure electronic identity credentials for use within particular social or economic domains

Registration empathetic and responsive

- Where Government is required to assess and decide eligibility for an ID credential, the registration process should, to the greatest possible extent, be localised and cooperative

Identity credentials revocable

- Technology should be employed to ensure that a biometric or an identity credential that has been stolen or compromised can be revoked

Identity numbers invisible outside the identity management system

- Any unique code or number assigned to an individual must be cryptographically protected and invisibly embedded within the identity system

Competition between operators and technologies

- Inter-working of multiple identity technologies run by multiple identity providers must be enabled technologically and legally

Consistent user experience

- Users should be able to enjoy a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

---

[53] Distilled from:
'Proof of ID required? Getting Identity Management Right', by Malcolm Crompton when Privacy Commissioner, March 2004 – in HTML, PDF or Word;
'Microsoft Laws of Identity' by Kim Cameron, May 2005 at http://msdn.microsoft.com/library/en-us/dnwebsrv/html/lawsofidentity.asp?frame=true&_r=1;
'The Identity Project: an assessment of the UK Identity Cards Bill and its implications' by London School of Economics, June 2005 at http://is.lse.ac.uk/idcard/identityreport.pdf