



**INFORMATION  
INTEGRITY  
SOLUTIONS**

## “Trust, Identity and Connected Government”

The Evolution of e-Government – From Policy to Practice

A Forum for the Research, Development and Evaluation  
Commission

**Malcolm Crompton**

Managing Director, Information Integrity Solutions Pty Ltd;  
Federal Privacy Commissioner of Australia, 1999-2004

[www.iispartners.com](http://www.iispartners.com)

Taipei

24 June 2005

## Introduction

### The challenge: Trust

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<sup>1</sup>. Both the Yankelovich and Westin<sup>2</sup> surveys, 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%.<sup>3</sup>

Financial institutions face additional challenges such as:

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

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<sup>4</sup> 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.<sup>5</sup>

Governments face the same challenges of trust in regard the services that they provide themselves. A US survey in 2003 found that 22% of those surveyed say that “they are not confident about protection of their privacy online, and 20% reporting that they are not confident that the Internet is secure”. As such, privacy is the second highest reason given for not using online government services more often, just after “cannot find the right website”. A major project by the UK Cabinet Office in 2002 also recognised the crucial role that respect for personal information and trust played in governments being permitted by their citizens to collect and share personal information, even though it is also crucial for the ‘joined up government’ that people also increasingly expect<sup>6</sup>.

In short, trust is a two way challenge, yet most organisations think only about when they can trust others.

---

<sup>1</sup> 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](http://www.privacy.gov.au/business/research/index.html)

<sup>2</sup> *The State of Consumer Trust Report*, Yankelovich Partners, [www.yankelovich.com](http://www.yankelovich.com), available online at [www.compad.com.au/cms/prinfluences/workstation/upFiles/955316.State\\_of\\_Consumer\\_Trust\\_Report\\_-\\_Final\\_for\\_Distribution.pdf](http://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](http://www.pandab.org) at [www.pandab.org/pabsurvey04pr.html](http://www.pandab.org/pabsurvey04pr.html)

<sup>3</sup> 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](http://www.computerworld.com/printthis/2004/0,4814,98448,00.html)

<sup>4</sup> See, for example, the FAQ *What is the Australian government doing to stop spam?* It has been issued by the Australian Communications Authority, online at: [http://internet.aca.gov.au/ACAINTER.65650:STANDARD:472427662:pc=PC\\_2935](http://internet.aca.gov.au/ACAINTER.65650:STANDARD:472427662:pc=PC_2935)

<sup>5</sup> See, for example, “Data leaks stunt e-commerce, survey suggests”, MSNBC, 15 June 2005 online at: [www.msnbc.msn.com/id/8219161/](http://www.msnbc.msn.com/id/8219161/)

<sup>6</sup> “The new E-Government equation: Ease, Engagement, Privacy and Protection”, Hart-Teeter Research, April 2003, online at [www.excelgov.org/usermedia/images/uploads/PDFs/egovpoll2003.pdf](http://www.excelgov.org/usermedia/images/uploads/PDFs/egovpoll2003.pdf); “Privacy and data-sharing: The way forward for public services”, UK Cabinet Office Performance and Innovation Unit, online at: [www.number-10.gov.uk/su/privacy/index.htm](http://www.number-10.gov.uk/su/privacy/index.htm) and the detailed supporting survey online at: [www.number-10.gov.uk/su/privacy/papers/perri6.pdf](http://www.number-10.gov.uk/su/privacy/papers/perri6.pdf)

# Trust, Identity and Connected Government

---

## Is Identity Management the solution?

Identity management is often seen as the key to improving trust and customer service. However, ID management can only do this if it succeeds in building two way trust and is not perceived as yet another policing action. The challenge is even greater if the customer believes that ID management will put all the powers and discretions in the hands of the institution to collect more personal information which it can then link, use, or disclose at its discretion.

This paper looks at the challenge of designing trustworthy identity management arrangements and the role that governments can play in responding to that challenge. The paper draws heavily on work undertaken while I was Federal Privacy Commissioner of Australia.<sup>7</sup>

## Identity management and privacy: playing for high stakes

Identity management<sup>8</sup> is proposed as a solution to a loose collection of issues with powerful economic, political and social resonance. Greater confidence about the identity of individuals, particularly in electronic contexts, is aimed at preventing financial, welfare and benefit fraud, protecting national borders and increasing national security, as well as better profiling customers or clients to better target services and goods.

Individuals themselves see a need to consolidate or simplify the way they present their identities to the world. Many of us can imagine how much more convenient it would be to have fewer PINs, passwords and plastic cards, for example. Many of us find the evidence of identity demands when we first deal with a government department or financial businesses, for example, to be onerous and intrusive.

The common thread, between individual and organisational needs for better identity management, is trust. Organisations want to trust the individuals they deal with; trust that they are who they say they are, and that they are authorised to do what they do. Individuals want to be trusted, but they also need to trust organisations to deal with them fairly, and to deal appropriately with their personal information.

Trust can be subtle, and can change over time. As I get to know you and to like you, I will trust you more. If you surprise me in a way that seems to betray that trust, I will be very wary of dealing with you in the future. Trust may be enhanced between us if there is a family connection or we come from the same region. As we will see, the nature of trust is just one of the reasons why identity management or, more accurately, good identity management, is a subtle business.

Implemented poorly, identity management is likely to be a cure much worse than the disease, posing risks to the fabric of our society, as well as having limited success in its goals of building trust, improving security, reducing fraud, and so on. Implemented well, identity management can achieve its goals without endangering personal freedom and privacy.

The widespread implementation of lazy identity management solutions – a real risk – would make it technically easy to combine vast amounts of electronic information held about a person, wherever it is stored, without that person's knowledge or permission and actually facilitate, instead of prevent, identity fraud.<sup>9</sup>

---

<sup>7</sup> In particular, this paper draws upon the paper "Proof of ID required? Getting Identity Management Right", Office of the Federal Privacy Commissioner, March 2004, online at: [www.privacy.gov.au/publications/index.html#S](http://www.privacy.gov.au/publications/index.html#S)

<sup>8</sup> "Identity management" is a relatively new term whose meaning may not be entirely settled, however for purposes of this paper we can understand identity management as a set of data management systems and practices designed to increase confidence in the identity of individuals where appropriate.

<sup>9</sup> See for example the evidence given by staff of the Attorney-General's Department to the House of Representatives Standing Committee on Legal and Constitutional Affairs during its Inquiry into Crime in the Community, Proof Committee Hansard, 26 September 2002, page LCA11 et seq.

# Trust, Identity and Connected Government

---

Think of all the information about each of us, both current and historical, that is presently stored electronically: taxation records, banking, finance and mortgage information, health records, household details such as who we phone, and what bills we pay, details of government benefits, where we live and how much we pay for it, shopping habits and employment details.

Then add the opinions, assessments and conclusions that are often recorded with this data, some of which may be little more than personal opinion.

Think now of how it would feel to have all this information collected together, available for interested parties (whether government agencies, law enforcement agencies, or businesses) to peruse, or data mine, at will, perhaps taken completely out of context.

Move beyond that, and imagine that this information is inappropriately accessed or is stolen. Once compromised, your whole world could be opened wide to scrutiny.

Poor identity management solutions could amount to almost total surveillance of some, if not all, individuals.

## ***What is identity?***

To investigate and understand identity management, however, it is first important to understand the more basic, but perhaps more difficult, concept of identity.

“Identity,” in its simplest sense, is the relationship between something and itself; it is the relation of being the same thing. We can call this “bare identity.” The term “identity”, however, has come to mean something more – my identity is something intrinsic to me that distinguishes me from others; it is my uniqueness, perhaps my set of core values, perhaps something about my social and cultural background. In short, my “social identity”.

Social identity is a complex, multifaceted notion. Each of us has a range of different identities defined through relations with others, position, status, actions, behaviours, characteristics, attitudes and the circumstances of the moment.

Control is a central feature of privacy. Its importance is illustrated in the nomination of “whether attention is paid” as a critical aspect of privacy – the actions of others in paying attention may be beyond our knowledge or control. Simply being watched, covertly, is a breach of one’s privacy.

## ***What is identity management?***

Those interested in managing identity are, first of all, interested in bare identity – they want to be sure that when they deal with me today online, they are dealing with the same person they dealt with last week face-to-face, and that this is the same person they are to deal with on the phone next week. From there, they may want to go on and develop a deeper understanding of my identity.

Identification is the action of being identified, of linking specific information with a particular person. An individual’s identity has a degree of fluidity and is likely to change over time. The extensive linking of different information about an individual may restrict or limit this fluidity. Moreover, new technologies often run against one of the subtle fundamentals of a healthy society – the ability to ‘forgive and forget’. To allow for growth and development, individuals need to be able to let life flow by. Few of us would want to be defined forever by all the attitudes we may have held at the age of 17.

Identification can potentially relate to a wide range of elements of an individual’s identity. In practice, identifying an individual generally involves focusing on those things that distinguish that individual from

## Trust, Identity and Connected Government

---

others including, legal name, date of birth, location or address and symbolic identifiers such as a driver's licence number. The basis for identifying a person can also involve such characteristics as:

- the person demonstrating that:
  - they have knowledge of something (e.g. a password); or
  - they possess a token (e.g. driver's licence); or
- a person's physical appearance, actions or characteristics (e.g. facial features, signature, fingerprint); or
- social characterisation (e.g. gender, ethnicity, education, employment and leisure activities).

One of the impacts of new technologies is the emergence of 'identity creep' or the capacity for gradual identification of 'non-identified' information through data mining or linkages of data.

### Assertions other than identity

Identity is only one of many assertions that may need confirmation. Organisations may wish to confirm a number of assertions I make, for example "I am Malcolm Crompton," or "I am the Federal Privacy Commissioner," or "I am licensed to drive a car," or "I am a doctor," or "I am transferring \$25 to pay for this item," or "I am authorised to operate this account," or "I am entitled to be in this building".

The point to recognise is that to date we have got along, being trusted in making many of these assertions, without identifying ourselves (or by identifying ourselves without strong proof). For example, on the vast majority of occasions where I have paid cash for goods, the transaction has been anonymous. On other occasions, the vendor may know my name (the local café owner greets me personally), but has no need for strong evidence that that really is my name. On yet other occasions the shop may have my name and address (perhaps stored on a warranty card), but it is kept in a manner that makes it actually quite difficult to link me to that transaction, except in the appropriate circumstances (for example, product recall).

What we are starting to see is increased pressure not only to identify ourselves for more and more of the transactions that make up our daily lives, but to show strong, verifiable evidence of our identities, in more and more of these transactions. If, in the future, we can only make these sorts of assertions by also identifying ourselves, and doing so in ways that make it easy to connect all the information surrounding those assertions, then our ability to lead our lives free of continuous close surveillance will be significantly compromised.

While in many circumstances organisations are primarily interested in the bare identity relationship – they want to confirm only that they are dealing with the same person that they dealt with last time – the way they seek to confirm that identity intrudes upon that identity in the second sense –social identity. The standard techniques for confirming bare identity (described later) often require us to reveal more information about ourselves than may be comfortable, and they also facilitate the greater spread and aggregation of information about ourselves.

### Drivers for ID management

There is increasing concern about the incidence and extent of identity fraud, where individuals create partially or entirely false identities in order to commit a fraud or other crimes. For example, by inventing a false identity, or obtaining or forging identity documents that relate to that identity, it is possible to claim government benefits fraudulently in the name of the false identity. Similarly, bank accounts opened under false identities provide a means to launder money. A recent report estimates the cost of

# Trust, Identity and Connected Government

---

identity fraud in Australia to be \$1.1bn per annum.<sup>10</sup> The report takes the view that “while the fraudulent representation of identity has existed for many decades, if not centuries”, it may be easier to perpetrate due to the rapid global information flows, increased use of the internet, and fewer face-to-face transactions.<sup>11</sup> Law enforcement officials argue that criminals, including organised crime, are increasingly looking to identity fraud because it is easier to perpetrate than more traditional theft, the rewards can be higher, and the consequences of getting caught are less.

Identity fraud is also considered an important factor in border control and traveller identification, where there is concern that individuals may be crossing borders under false pretences. The then Minister for Immigration, Multicultural and Indigenous Affairs argued that “identity and document fraud facilitates the movement of terrorists and transnational crime to Australia.”<sup>12</sup>

The increasing complexity of IT networks, where individuals may want to be authorised to access a number of different, but related, IT systems, is also driving a need for improved identity management. Recent federated identity initiatives are a response to this sort of demand.<sup>13</sup>

In the health sector, where health information is increasingly moving to electronic storage, it is argued that the introduction of a unique patient identifier may improve clinical care to the individual, by combining disparate sources of health information to form a comprehensive health record, and making the flow of potentially crucial clinical information between health professionals increasingly timely and efficient. According to the National Electronic Health Records Taskforce, the *HealthConnect* initiative alone is expected to achieve conservative savings of at least \$300 million per annum.<sup>14</sup> In addition, a unique patient identifier is hoped to facilitate greater efficiencies in the use of health resources, in particular by reducing duplication in testing and prescribing medicines

Finally, increased convenience and improved, better connected services have great potential consumer benefits.

## Authentication

The key to identity management is authentication, which often starts with a process of enrolment.

A simple model of identity management may involve the registering of a person with an organisation, followed by authentication of that enrolled identity on subsequent interactions.

In the old days of passbook bank accounts, for example, the enrolment phase would involve turning up to a bank branch in person, and providing details such as name and address. On enrolment, the bank would issue the customer with a passbook which included the individual’s signature.

Authentication of the identity of someone attempting to withdraw money would then take place by comparing the signature in the passbook to the signature of the individual withdrawing money. In this process, no other evidence of identity was required, and there was no method of checking whether you “really” were who you said you were. This could be said to be an example of ‘go forward’ enrolment –

---

<sup>10</sup> *Identity Fraud in Australia: An evaluation of its Nature, Cost and Extent* by Suresh Cuganesan and David Lacey. Standards Australia, Sydney, 2003. For more information see [www.sirca.org.au/news/releases/2003/0302FraudBook.html](http://www.sirca.org.au/news/releases/2003/0302FraudBook.html).

<sup>11</sup> *Identity Fraud in Australia*, p. 1.

<sup>12</sup> See the Minister’s Second Reading Speech in relation to the Migration Legislation Amendment (Identification and Authentication) Bill 2003, available at <http://parlinfoweb.aph.gov.au/piweb/browse.aspx?NodeID=1449>.

<sup>13</sup> See, for example, the Liberty Alliance home page at [www.projectliberty.org](http://www.projectliberty.org).

<sup>14</sup> See Department of Health and Ageing, *HealthConnect Interim Research Report Volume 1: Overview and Findings*, 2003, Executive Summary, p. 9, available at [www.healthconnect.gov.au/pdf/v1.pdf](http://www.healthconnect.gov.au/pdf/v1.pdf).

## Trust, Identity and Connected Government

---

we do not know who you are and nor do we need to, but we do have to authenticate that you are the same person when you come back. This is the quintessential 'Swiss bank account' model.

Often, though, what needs to be authenticated is a claim to an existing identity. At enrolment, the enrolling individual is claiming to be known by a certain name, to live at a certain address, and so on. These claims are authenticated by evidence of identity (EOI) documents that tie the person presenting the documents to the information on the documents, for example a birth certificate confirms that a person with that name was born at a certain place and a certain time; a driver's licence confirms that a person with that name, who looks like this photo, lives at a certain address, and was born on a certain date, and so on.

Once the individual has registered or enrolled with the organisation, these initial claims about name, address, date of birth and so on do not need to be re-authenticated. However, the organisation does need to satisfy itself that it is dealing with the same person who enrolled initially. That is, the organisation needs to authenticate the enrolled identity.

These two kinds of authentication of identity – at enrolment; and at subsequent interactions – are paradigm examples of identity management processes. The challenges that face organisations in this regard include ensuring that the individual registered is the same as the individual referred to on the evidence of identity documents; ensuring that the evidence of identity documents are genuine; ensuring that the person claiming to be an enrolled person is in fact that person, and so on.

Identity is not always the important thing to be authenticated, however. As noted earlier, assertions other than identity may also need to be authenticated. For example, traditionally, commuters have been able to travel on public transport without declaring their identity, or having it authenticated. Bus tickets, for example, may entitle the bearer to one, or ten, or a week's worth of bus rides. While the ticket may be authenticated (either manually by a person, or automatically by a machine), the identity of the person using the ticket need not be identified in order to travel.

### ***Dangers of poor identity management***

#### **The protection of "practical obscurity" disappears**

To appreciate the dangers of poor identity management, we need first to understand why the existing identity management processes, in combination with the wealth of personal information that is stored electronically throughout the public and private sectors, has not already led to significant privacy issues.

The present protections arise through a number of factors. There are explicit legal protections, including of course privacy laws.<sup>15</sup> The nature of the technology used to store and handle personal information also offers privacy protection. For example, data collected for a certain purpose is often kept in isolated "silos" and, given that accurate data matching is difficult, these silos cannot be easily merged together. More simply, personal information recorded on paper files is much harder to manipulate and integrate. Market forces play an important practical role in protecting privacy as well. Data matching is expensive and resource intensive, while consumer acceptance of existing identity management systems and processes may mean there is a degree of resistance to changing widespread identity management practices.

Further privacy protection arises from the simple fact that many organisations that hold personal information are unaware of its potential value, either to themselves, or to others as a commodity. Lastly, there are privacy protections provided through social norms: organisations and governments retain, to varying degrees, a culture of "custodianship" of personal information, recognising that they hold data that may be private.

---

<sup>15</sup> Information on Australian privacy laws may be found at [www.privacy.gov.au/act/index.html](http://www.privacy.gov.au/act/index.html). A more general survey is available from the Australian Privacy Foundation at [www.privacy.org.au/Resources/index.html](http://www.privacy.org.au/Resources/index.html).

# Trust, Identity and Connected Government

---

The net effect of all these protections – only a very few of which are designed to be privacy protections – is that identity management systems are slow to change, and that personal information is hard to integrate. This net effect has been termed “practical obscurity”.

Practical obscurity, however, is under pressure.

## Function creep

“Function creep” describes the gradual increase in the purposes for which information is used. It is common for data to be collected for one purpose, but, after a period of time, for the organisation holding the data to recognise other purposes for which the data can be used. Privacy legislation guards against function creep through “use-for-purpose” or “use limitation” principles that require that personal information that is collected for one purpose should not be used or disclosed for an unrelated purpose.

In the identity management arena, the use of the Tax File Number in Australia provides an example of function creep (and of the need for protections other than law). Tax file numbers (TFNs) are unique numbers issued by the Australian Taxation Office (ATO) to identify individuals, companies and others who lodge income tax returns with the ATO. TFNs are designed primarily to collect together the taxation-related information about each individual. There is a Voluntary Quotation Principle (Guideline 1.1 of the Tax File Number Guidelines<sup>16</sup>) by which quoting one’s tax file number is guaranteed to be voluntary. However, individuals who do not quote their TFN to employers and financial institutions have tax deducted from their income or interest payments at the highest marginal rate plus the Medicare levy.

When the Tax File Numbers first came into effect in 1988, for many people, the only penalty for not quoting it was that for some income, for example a dividend stream, you made an interest free loan for less than a year to the Tax Office of the difference between the top marginal tax rate and the marginal tax rate you paid (this amounted to nothing for high income earners and not much for most others).

Through a range of legislative changes since 1988, it is now the case that some Australians are not able to survive without obtaining and quoting their TFN (for example, to obtain unemployment benefits and a number of other interactions with Government). But the Voluntary Quotation Principle is still in place: if you are unemployed, you do not have to receive unemployment benefits, so you do not have to quote your TFN!

The function of the Tax File Number has moved from, as it was initially, a purely taxation-related function, to the present situation, where it is used to cross match data relating to government assistance of various sorts and superannuation.

Not only is the TFN story a good example of function creep, it also illustrates how privacy promises made in law can be lost over a very short period of time.

## Total surveillance

So what is wrong with being absolutely sure of identity? What is wrong with collecting reliable identifying information whenever possible? From the perspective of any particular project or organisation, the problems may not be obvious.

The danger is pervasive surveillance, which arises from widespread data linkage beyond the control of the individuals concerned. If more and more organisations collect more and more identifiable, linkable information about what we do, when, and with whom, then whoever gets to link all that information

---

<sup>16</sup> See [www.privacy.gov.au/publications/tfngls.pdf](http://www.privacy.gov.au/publications/tfngls.pdf).

## Trust, Identity and Connected Government

---

together – whether government or not – will have an enormous amount of knowledge of each of us individually, and through that knowledge, could change radically the fabric of society.

Think of the potentially identifiable information about each of us, increasingly being collected and stored every day: vehicle movements are tracked in a low resolution manner by automatic toll collection, and with much higher resolution by GPS tracking devices; phone calls, email and web traffic are listed and archived by telecommunication carriers; purchases are recorded by credit and debit card transactions; surveillance cameras increasingly cover more and more public and private space;<sup>17</sup> financial affairs are recorded by financial institutions, reported to government, and held by the tax office;<sup>18</sup> health data is held by Medicare and the public health system; life circumstance information is held by welfare and job-seeking agencies; employment records are held by employers; and the list goes on.

Add to that the publicly available information that anyone with an interest can collate together: telephone number and address; house sale price information; company share register information; etc.

Furthermore, in the online environment, audit trails and data trails add a further layer of data, documenting an individual's various interactions with the world. Where a token or identifier can be used to link these various trails back to one identity, an entirely new and rich data set is created about an individual. An example of such a data trail is the 'clickstream' data collected by some internet marketers through the use of cookies and web bugs. Such data can reveal that a person is, for example, a member of a trainspotting club, or has visited a particular sexual health information site: revelations that the individual may have preferred not be revealed.

Mostly, this information is only collected because it is required for some reasonable purpose (privacy law, where it exists, will impose this restriction). Data matching is still in its infancy, is still an art,<sup>19</sup> it is expensive and it is time consuming to undertake large scale data matching of disparate data sets not designed to be interlinked.

The central privacy risk to an incautious approach to identity management is that it will make the undesirable "zipping together" of all this data much easier. This privacy risk emerges in two forms. The first is the zipping together of data by organisations that have legitimately collected the data for other purposes.

The second form it takes is where the information is compromised, for example through hacking or computer theft, etc. Those who steal information with criminal intent may be able to do significant damage, whether by committing financial frauds such as credit card frauds, or through identity theft.

---

<sup>17</sup> For example, Britain is estimated to have 4,500 speed cameras, and more than 2.5 million CCTV cameras that catch each British resident as many as 300 times each day. See, e.g., "Smile, You're Being Watched: Brits take intrusive "security" measures into their own hands", MSNBC, 17 Oct 2003, available at [www.msnbc.com/news/981718.asp](http://www.msnbc.com/news/981718.asp).

<sup>18</sup> Australia will be implementing new global standards aimed at cracking down on money laundering and terrorist financing by putting into place the range of global anti-money laundering standards issued by the Financial Action Taskforce on Money Laundering (FATF), a 33-member international body of which Australia is a founding member. For the media release announcing this decision on the website of the Minister for Justice and Customs see [www.ag.gov.au/www/justiceministerHome.nsf/Web+Pages/448419DCA3156F1BCA256DF5007AC772](http://www.ag.gov.au/www/justiceministerHome.nsf/Web+Pages/448419DCA3156F1BCA256DF5007AC772). For the actual recommendations see [www1.oecd.org/fatf/pdf/40Recs-2003\\_en.pdf](http://www1.oecd.org/fatf/pdf/40Recs-2003_en.pdf). For further information on anti money laundering reform see [www.ag.gov.au/aml](http://www.ag.gov.au/aml).

<sup>19</sup> Note, for example, moves such as that by the fledgling Institute of Analytics Professionals of Australia, which is hoping that the creation of a data-mining certification will lead to the professionalisation of the data mining industry. See: "An analytical approach to data mining", *Sydney Morning Herald*, 9 March 2004 at [www.smh.com.au/articles/2004/03/08/1078594280704.html](http://www.smh.com.au/articles/2004/03/08/1078594280704.html).

# Trust, Identity and Connected Government

---

## ***Good Identity Management***

Good identity management involves processes that give confidence to the degree appropriate for the occasion that the organisation is dealing with the right person – but in a way that does not facilitate inappropriate, unnecessary data linkage. In particular, good identity management means only authenticating identity when it is absolutely necessary to do so.

In any attempt to describe and catalogue the fundamentals of good identity management, it is important to recognise that no particular approach, or technology, is of itself privacy enhancing. Only by carefully analysing the identity management system as a whole, is it possible to be clear about the overall privacy impacts.

Some of the characteristics of good identity management might include the following.

### **Multiple identities allowed**

It is commonly asserted, or implied, that individuals have only one ‘real’ or ‘true’ name. It might be thought that the full name that appears on a birth certificate, for example, is someone’s ‘real’ name.

In reality, however, most of us are known by a number of names and nicknames, and these may differ from context to context. Given that in the “real world” we are known by a range of names, and these different names may be associated with different social identities, identity management systems that force individuals to be known by only one, canonical name are forcing an arbitrary choice on individuals about their identity, including their self-identity.

As well as respecting the multiplicity of real world identity, allowing individuals to adopt multiple identities prevents a drift to one number per person systems, and adds another layer of practical obscurity by acting as a natural (but not insurmountable) barrier to function creep and inappropriate data linkage and aggregation.

### **Consider authenticating identity last**

Putting together two earlier considerations – first, that often identity is not the key feature that needs to be authenticated; and secondly, that excessive collection of identifying information is a growing privacy and security risk – leads to the conclusion that identity management systems should only ever authenticate identity, as opposed to the other aspects of an individual or a transaction, once it has been shown that this is necessary.

Designers of identity management systems should carefully consider whether authentication of identity is indeed necessary to meet their core objectives. If not, then identities should not be authenticated.

Note that choosing not to authenticate identity is not the same as dealing with individuals anonymously. In many circumstances it will be appropriate to use someone’s name as part of the organisation’s dealings with that person. The key privacy protection being emphasised here is that of not going to lengths to check that the name provided matches some other list of names. If identity does not need to be authenticated, then it does not matter whether you deal with someone using their first name only, or a nickname, or an unmarried name, or anglicised name, and so on. This sort of flexibility in identifying individuals using the name they choose is one small step towards building the trust of individuals by respecting their privacy and offering them a degree of control over the management of their identity.

To take a simple example, registration forms for free internet services such as online newspapers often ask for a name. It does not actually matter what name is entered, because it does not need to be authenticated. The purpose of registration is to collect demographic and marketing information about the site’s visitors, and to tailor the viewing experience for the individual. The purpose of requiring the logging in procedure is to authenticate that the *same* user is now browsing, as was browsing before. The name of the user is not actually required.

# Trust, Identity and Connected Government

---

## Individuals retain control

As we have discussed, the sense of control we have about who we are and what is known about us is central to our sense of privacy. Identity management systems that reduce this level of control, particularly when the reduction in control is arbitrary or unnecessary, are failing the privacy test.

Of course there are always limits to the amount of control individuals have over their identity and their personal information, so it is not as though individual control is absolute. Privacy issues arise when a reasonable level of control is denied.

In identity management systems, individuals should have as much control as possible over names and other identifiers.

## Unique identifiers specific to application

A significant, and straightforward, privacy risk comes about if all the databases use the same number to identify each individual. A similar privacy risk arises simply if databases keep a record of the unique identifier of other databases.

To protect against this privacy risk, the solution is to ensure that different data sets use different identifiers. This idea is now reflected in legislation, for example in National Privacy Principle 7 in the Australian Privacy Act. The value of this protection is that it makes data matching more difficult.

Of course, there may be legitimate reasons to match data – sometimes on a regular basis, sometimes on a once-off basis. But these situations should be the exception, not the norm, and should be known, publicly justified and be based wherever possible on the consent of the individuals involved.

There are a number of technical approaches that can deliver this sort of outcome. A simple requirement would be that different databases issue different ID numbers.

A more sophisticated approach might make use of a family of related identifiers for each person. For example, imagine a situation where there are two databases that may need to be linked under special circumstances, but for day-to-day purposes they contain personal information collected for different and unrelated purposes. Imagine that for each individual, their identifier in the first database is a different number to that in the second database. However, armed with special knowledge, these two identifiers can be linked. It may be that one is a particular permutation of the other – once a data manager knows the permutation, then the data can be linked. While this may seem to be introducing complexity, the point of this sort of system is to design into the system a clear control point: whoever has the knowledge about how to link the two identifiers, has control over the linking of that information.

If the individual is the only person who can provide the information about how to link the identifiers, then the individual has control over the linking of that information. Alternatively, it may be that an appropriately senior judicial or similar authority is required to unlock the information about how to link the data.

## Identifiers carry no information

The increasing popularity of biometric identification systems offers both privacy dangers and potential privacy benefits. The numbers traditionally used as unique identifiers in databases typically have the benefit of being arbitrary – potentially, the number itself tells you nothing about the individual, it is only a pointer to information about the individual stored in the database.

Biometric identifiers, however, can carry out two roles at once. For example, a complete DNA sequence might operate as a unique identifier – no-one (other than an identical twin) should have the same DNA sequence as me, so using a numerical representation of my DNA as a database identifier would be an ideal unique identifier for a database. Indeed, one of the things that make biometric

## Trust, Identity and Connected Government

---

identifiers attractive is precisely that they are not arbitrary – the unique ID in the database can only relate to me; an arbitrarily assigned number could have been assigned to anyone.

A significant privacy downside of some biometric identifiers, however, is that they carry a lot more information than does an arbitrary number. My full DNA sequence says an awful lot about my genetic heritage, my predisposition to health and disease, about gender, race, and so on.

Even the kind of DNA analysis commonly used for forensic DNA profiling and matching, which was designed to look at so-called “junk” DNA for identifying purposes, is turning out to carry information about individuals. While “junk” DNA was long regarded as containing no phenotypical information, science is recently suggesting otherwise. Research has shown that standard DNA fingerprints used by police around the world contain a subtle signature which can be linked to a person's susceptibility to type 1 diabetes.<sup>20</sup>

Similar concerns may arise with other biometric identifiers. Facial biometrics, particularly in the form of digitised pictures, obviously carry a lot of information beyond a mere number as they tell us how a person looks. A person's voice carries with it information about accent, and possibly cultural background. Generally speaking, there seems a risk that any unique number generated from a body may carry more information about that body than simply identity. As the case of DNA identification shows, at the time of collection, scientists may not have been aware of the potential of the biometric identifier to carry other information.

This leads to another element of privacy protection: that whatever identifiers are used, they should carry no information about the individual beyond bare identity.

Many biometric systems make use of a biometric template – a mathematical representation of the biometric feature whose structure reflects the aspects of the biometric feature relevant to its use as an identifier or match key. So a fingerprint scanner may take an electronic photograph of a fingerprint, then process that picture to produce a number or string of numbers, called the biometric template. The template is therefore distinct from the fingerprint itself. In some cases, it is possible to reconstruct the biometric feature (e.g. a picture of the fingerprint) from the template, in others it is not. Since all that is required for the identity authentication job is the biometric template, then the best approach to storing biometric is to store templates from which the biometric features cannot be reconstructed.

This approach has the advantage of using identifiers that carry less information about the individual, and may have a security benefit because the ability to reverse engineer a biometric from a template may give rise to counterfeit biometrics. For example, it has been reported that a Japanese researcher, making use of a fake finger created with gelatine, defeated 11 different commercial fingerprint readers<sup>21</sup>

## Data silos

Remembering that data linkage is a key privacy risk to be managed in implementing new identification and authentication systems, then a third privacy protection is to encourage unrelated data to be stored separately. Data silos might sometimes be the bane of the datamatcher; but they can be the friend of privacy.

---

<sup>20</sup> See “Fingerprint Fear”, New Scientist, 2 May 2001, at [www.newscientist.com/news/news.jsp?id=ns9999694](http://www.newscientist.com/news/news.jsp?id=ns9999694). See also Cherfas, J. (2002) *The Human Genome* p. 49. London: Dorling Kindersley, and “One man's junk is another man's treasure”, Sydney Morning Herald, 9 July 2003, at [www.smh.com.au/articles/2003/07/08/1057430206624.html](http://www.smh.com.au/articles/2003/07/08/1057430206624.html).

<sup>21</sup> See: “Jelly babies dupe fingerprint security”, ZDNet, 17 May 2002, at [www.zdnet.com.au/news/security/0,2000061744,20265318,00.htm](http://www.zdnet.com.au/news/security/0,2000061744,20265318,00.htm).

# Trust, Identity and Connected Government

---

There may also be sound business reasons for keeping unrelated data separate. Aggregation of data into a single big database magnifies the risks by concentrating all the value into one place, leading to what we might call the “Fort Knox” problem.<sup>22</sup>

## De-identification

Data managers see a lot of value to their organisation in the data they hold. Statistical analysis of aggregate data can tell an organisation a lot about its processes, its clients or customers, and so on. Again, though, thoughtless analysis fails to see the difference between wanting to understand population behaviour and to understand or track individual activity. More often than many would admit, the real goal is understanding and predicting population behaviour is all that is needed.

There is rarely any need to use identified data for this sort of statistical analysis. If identified data is not needed, then it is wise to de-identify it as thoroughly as possible. Privacy-preserving data mining techniques have already been developed to allow data mining to be conducted in this way.<sup>23</sup>

When considering de-identifying data, it is important to note that simply removing the person's name may not be enough. In some circumstances a person's identity may reasonably be ascertained from other information – for example from an identifier, or other details held about the person, or from the context in which the information is collected.

## Summary of good identity management:

In summary, then, a good identity management solution is one in which, except where absolutely necessary, or where the individual wants it otherwise:

- multiple identities are allowed;
- identity is not authenticated;
- individuals retain control over their identities, their identifiers, and the associated personal information;
- any unique identifiers used in the system are specific to that system and not interoperable with other systems;
- any unique identifiers used in the system carry no information about the individual;
- personal information collected for disparate purposes is kept unlinked and unlinkable; and
- information is de-identified before being used for secondary purposes.

The net effect of these parameters is that individuals retain an appropriate degree of control over how they present themselves to the organisations with which they deal, and regarding how information about them is handled. Removing from individuals, control over how they are identified and named risks losing their trust.

---

<sup>22</sup> Like the story in Ian Fleming's ‘Goldfinger’, locking up all the world's gold in one place, Fort Knox, only results in increasing the incentive to successfully break into it.

<sup>23</sup> “‘DB2 Anonymous Resolution’ Announced by IBM”, ebizQ, 24 May 2005, online at

[www.ebizq.net/news/5966.html](http://www.ebizq.net/news/5966.html); see also

“IBM Scientists Rely on the Principle of Uncertainty To Develop Web-Privacy Answers”, IBM Press Release of 23 May 2002, available online at:

[www-](http://www-1.ibm.com/press/PressServletForm.wss?MenuChoice=pressreleases&TemplateName=ShowPressReleaseTemplate&SelectString=t1.docunid=703&TableName=DataheadApplicationClass&SESSIONKEY=any&WindowTitle=Press%2BRelease)

[1.ibm.com/press/PressServletForm.wss?MenuChoice=pressreleases&TemplateName=ShowPressReleaseTemplate&SelectString=t1.docunid=703&TableName=DataheadApplicationClass&SESSIONKEY=any&WindowTitle=Press%2BRelease](http://1.ibm.com/press/PressServletForm.wss?MenuChoice=pressreleases&TemplateName=ShowPressReleaseTemplate&SelectString=t1.docunid=703&TableName=DataheadApplicationClass&SESSIONKEY=any&WindowTitle=Press%2BRelease)

A more detailed exposition, “Privacy-Preserving Data Mining: A Randomization Approach” is available online at: [www.almaden.ibm.com/institute/pdf/2003/RamakrishnanSrikant.pdf](http://www.almaden.ibm.com/institute/pdf/2003/RamakrishnanSrikant.pdf).

## ***Is good identity management technically feasible?***

In today's world, the answer is unequivocally yes. This point does not need to be developed further here. However, for those who are interested, examples of technologies that can deliver the features of good identity management are set out in the Appendix to this paper.

## ***Achieving good identity management***

### **What does success feel like?**

The key markers of success from an individual's perspective are control and trust.

An identity management system is successful to the extent that the individuals whose identity is "managed" retain an appropriate degree of control over what is personal to them. For example, where individuals identify themselves when *they* feel it is appropriate, and provide the strength of evidence *they* feel is appropriate in the situation, they are likely to retain what *they* think is an appropriate degree of control over their information. There may be occasions where individual control needs to be overridden, however these should be minimised, thoroughly justified and often regulated in law. While we need to recognise that an important part of the ongoing identity management debate will arise from the need to balance individual control with other important factors, we must not lose sight of the critical importance of maintaining individual control to the maximum extent possible.

The mechanism for achieving individual control can differ according to context. In some contexts it may be appropriate for individuals to be able to exercise a fine-grained degree of choice about exactly what information about them is used when, where and by whom. For some people, particular aspects of their medical history, such as sexual health, might fall into this category. In other contexts, where individuals understand the need for information to be provided, even if they have no choice in providing it, they can appreciate that the information is only being used for a specific purpose. Feeling in control, in an overall sense, does not necessarily mean having total, fine-grained control over every aspect.

Where individuals feel they have to identify themselves too often, without good cause, and to "prove" their identity to the satisfaction of others, they are likely to question where the information about them, their behaviour, and their identity, is going to, and how it is to be used. Indeed, there is clear evidence that they respond subversively.<sup>24</sup>

So individuals need to feel in control, but not necessarily total control, of the information about them that is collected and handled.

Which brings us to the second marker of success, from the perspective of individuals, which is trust, and it has two facets in this context.

First, individuals want to be trusted. It is exhausting, embarrassing and insulting to go through life mistrusted. Frequently having to justify yourself to others, frequently having to prove that you are who you say you are, frequently having to explain just why it is you are permitted to do what you are doing, is alienating. The more that organisations, governments and other individuals mistrust us, particularly on

---

<sup>24</sup> For example, surveys on community attitudes to privacy in Australia, have found that a number of respondents admitted that they provided false information when completing forms over the internet. See *Privacy and the Community*, prepared for the Office of the Federal Privacy Commissioner, prepared by Roy Morgan Research, in 2001 and 2004. Available online at [www.privacy.gov.au/publications/rcommunity.html#4.31.3](http://www.privacy.gov.au/publications/rcommunity.html#4.31.3) and [www.privacy.gov.au/publications/rcommunity/chap10.html](http://www.privacy.gov.au/publications/rcommunity/chap10.html). Another example is a survey done by the Californian HealthCare Foundation, where approximately one in six respondents reported that they had "done something out of the ordinary to keep personal medical information confidential". See "Americans Worry about the Privacy of Their Computerized Medical Records", 28 January 1999, available online at [www.chcf.org/press/view.cfm?itemID=12267](http://www.chcf.org/press/view.cfm?itemID=12267).

## Trust, Identity and Connected Government

---

those things that are central to who we are, the more we will feel alienated from those organisations, from government, and from each other.

On the other hand, the more I trust an organisation, the more information about myself I am likely to share with that organisation. Organisations that make a conscious effort to build trust and foster individual control are likely to increase the quality of the personal information, including identifying information, that they hold.

Secondly, individuals need to trust organisations to handle properly, the personal information held about them. Giving up personal information is not only inevitable in society, it is absolutely essential to a healthy life. But where we give up information about ourselves, or our families – information that may be sensitive in nature – or simply private; then we want to trust the recipient of the information not to misuse the information. The very difficult challenge faced by the drafters of privacy laws and regulations is that “misuse” is very hard to pin down. Appropriate and inappropriate use of personal information can differ significantly from context to context, depending on the nature of the information itself, the nature of the recipient, why it was given up, or collected, in the first place, and so on.

The key problems identified here – individual lack of trust, and of control – are to a significant degree problems of aggregation. It is the widespread, pervasive lack of trust and lack of control that will present, ultimately, as a profound problem for society. Each individual step along the way; a new smartcard for this, a new identity scheme for that, will not, of themselves, give rise to the alienation and disconnection I am suggesting. But taken in aggregate, over time, they could pose a serious issue. This means that policy makers have a special obligation to look beyond any particular identity management initiative, to appreciate the growing trend toward stronger and more pervasive identity management, and factor that growing trend into their policy making.

From the perspective of organisations, the key markers are trust and efficient data management.

Organisations have a successful identity management system when they trust the data they hold, and trust the individuals and other organisations with which they deal. As discussed earlier, trusting individuals does not always mean knowing exactly who they are. For cash transactions, the cash provides all the trust that is required. For other transactions, individuals may provide a name, but if the identity of the person is not material, then there is no need to require evidence of identity. In short, establishing the required trust depends critically on the specifics of the situation. Very often, the trust to be established relates to value, or credential (authorised plumber, licensed driver, etc.) rather than identity as such.

A key test for success will be whether identifying information is being collected to guard against the possibility of fraud or of the transaction being repudiated in some way. If, after careful analysis, the transaction in question requires only that certain non-identity aspects of the individual be authenticated (e.g. that she is licensed to drive, and that she has paid for the hire of the car), then the authentication of the driver's identity, “just in case” the organisation needs to track down payment, signals a failure in the systems to authenticate the real issues (that is, licensed to drive, and payment).

This is a challenging suggestion, not least because it is natural when dealing with people to want to know their names. As I have argued, however, there is a key difference between knowing a name, and authenticating that identity in a strong and robust manner. If, in renting a car, all the car rental company needs is to reliable evidence the renter can drive, and non-repudiable payment, then these are the only information items that need to be authenticated with high reliability. The renter may offer her name, and it may be recorded simply for the purpose of dealing politely with her; but the name need not be authenticated, and may not even need to be stored at all. The renter may simply offer her first name, or a nickname, and there would be no need to ask further.

# Trust, Identity and Connected Government

---

## The right approach

How, then, does an organisation faced with significant identity management challenges, ensure that it implements the right kind of solution? How do governments, businesses and the society more broadly work together to ensure that all the many identity management solutions being implemented at every different level – from small group of customers to the whole population – do not, in combination, give rise to unforeseen privacy consequences?

In short, the answer is to invest the right amount of energy into analysis and planning.

As Privacy Commissioner, I proposed a framework to assist in ensuring that the measures do not unduly affect the privacy of individuals. The framework – the AAAA framework – also has application in situations where identity management pressures are building.<sup>25</sup>

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.<sup>26</sup>

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

**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?

In considering identity management projects where the potential for function creep and unplanned data linkage is ever present, it is critical that the scope of the identity management system is carefully designed and constrained. Not only must the analysis be carefully undertaken to ensure that that identity management solution is fit for purpose (for example, the system only authenticates the identity individuals where it really has to, the system uses its own specific identifiers, etc.), there need to be structures in place that ensure that the scope of the system is retained into the future.

These structures need to include a combination of law, technology, and accountability. New systems that may pose a privacy risk can include promises of various sorts that the system will not be implemented in a privacy-invasive way. These privacy promises may occur in guidelines for the operation of the system, or in standards that that the system meets, or, most impressively, in law or

---

<sup>25</sup> This approach derives from the “AAAA framework” developed by the OFPC for the purpose of assessing and implementing new law enforcement and national security powers. Earlier versions of this framework were first outlined in an OFPC 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](http://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](http://www.privacy.gov.au/publications/secleg.doc)).

<sup>26</sup> Some guidance on matters that might need to be considered when conducting a Privacy Impact Assessment (at least in the context of government agencies) is available as Appendix 1 to the Office’s paper released in 2001 entitled “Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals”: see our website at [www.privacy.gov.au/publications/pki.pdf](http://www.privacy.gov.au/publications/pki.pdf). The Office also released in 2004 a “Consultation draft of Managing Privacy Risk – An Introductory Guide to Privacy Impact Assessment for Australian Government and ACT Government Agencies”, online at [www.privacy.gov.au/publications/mprdraft.pdf](http://www.privacy.gov.au/publications/mprdraft.pdf). The draft Guide incorporates, as an attachment, a draft “Privacy Impact Checklist” (PIC) developed by the Attorney-General’s Department, in consultation with the Office, online at [www.privacy.gov.au/publications/picdraft.pdf](http://www.privacy.gov.au/publications/picdraft.pdf). For more background, see [www.privacy.gov.au/government/officers/news/index.html](http://www.privacy.gov.au/government/officers/news/index.html).

## Trust, Identity and Connected Government

---

regulation (for convenience, I will refer to these kinds of structures as “law”). It is the nature of such promises, however, that they can be amended, or rescinded, as circumstances change.

We saw earlier that the structure of the Tax File Number system in Australia that was clearly set out in law, over a period of just a few years moved from incorporating genuinely voluntary use of the Tax File Number, to a situation where for many individuals quotation of the Tax File Number is effectively mandatory.

Laws protecting the privacy promise are nonetheless necessary, to clearly state the intended parameters of the system. But law that ignores the realities of marketplace and technological development will have little impact.<sup>27</sup>

The law alone cannot ensure that the right balance, however. A more convincing privacy promise can be made when the technology that implements the new systems is designed so that the privacy promise is “built-in”. In such system, overcoming the privacy promise requires not only changing policy, but re-engineering and other costs.

Even the powerful combination of law and technology is not enough to make a convincing privacy promise when implementing powerful new identity management solutions. The more powerful, or potentially invasive, the system, the greater the importance of a robust accountability system. Regardless of how good these protections are, all systems fail. This may happen because of human error, deliberate hacking, simple power failures or any number of other reasons. This is a certainty and a fact. Risk prevention and mitigation strategies are also therefore essential. Hence, transparency is a particularly important element of accountability in systems with privacy impacts. One of the key privacy principles enshrined in privacy laws throughout the world is the access principle: individuals should be able to know what information about them is held by organizations. This access right is central to the sort of transparency required of identity management systems. In combination with independent complaints handling and independent audit processes.

It is the overall combination of legal and policy frameworks, delivered through privacy-enhancing technology, under a transparent and accountable system, that can provide a trusted approach to identity management.

We have already discussed the requirements of a good identity management solution. Wherever possible, these parameters are fixed through technological design and implementation, are promised through law, standards, or other policy commitments, and adherence to these parameters is ensured through appropriate mechanisms of transparency and accountability.

### ***A role for government***

Governments in our region are 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.

Some economies in the Asia-Pacific region have had broad based privacy law in place for some years, including Hong Kong<sup>28</sup>, New Zealand<sup>29</sup>, Australia<sup>30</sup> and Canada<sup>31</sup>. Other economies have introduced

---

<sup>27</sup> See Joel R. Reidenberg, “Privacy Protection and the Interdependence of Law, Technology and Self-Regulation”, available online at <http://reidenberg.home.sprynet.com/Interdependence.htm>.

<sup>28</sup> *The Personal Data Privacy Ordinance*; see [www.pco.org.hk](http://www.pco.org.hk)

<sup>29</sup> *Privacy Act 1993*; see [www.privacy.org.nz/top.html](http://www.privacy.org.nz/top.html)

<sup>30</sup> *Privacy Act 1988*; see [www.privacy.gov.au](http://www.privacy.gov.au)

<sup>31</sup> *Privacy Act 1980 and Personal Information Protection and Electronic Documents Act 2000*; see [www.privcom.gc.ca/index\\_e.asp](http://www.privcom.gc.ca/index_e.asp)

# Trust, Identity and Connected Government

---

such laws more recently, with privacy law in Japan commencing on 1 April this year.<sup>32</sup> The United States of America has taken a route that is different again, with many sectoral or specific laws in place.<sup>33</sup> Korea also has sectoral law<sup>34</sup> 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.<sup>35</sup>

More specifically, many governments have sought to facilitate improved identity management systems. Examples of better, more privacy respecting approaches include the initiatives in Sweden<sup>36</sup> (generally considered to have the best eGovernment initiatives in Europe<sup>37</sup>), Austria<sup>38</sup> and New Zealand.<sup>39</sup> 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.

One of the better government sponsored research programs into identity management is PRIME, the Privacy and Identity Management for Europe project.<sup>40</sup> This program has multiple, privacy enhancing objectives but chief among them is that in addition to ensuring multiple identities, it also provides for 'trusted pseudonymous transactions'. In particular, this means that the entity that authenticates an assertion about identity is not able to find out either who is asking for the authentication or about whom the question is being asked. It is based on the Zero-Knowledge proofs that have been available for some years now.

## 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

---

<sup>32</sup> *Personal Information Protection Act*; see [www.privacyexchange.org/japan/japanindex.html](http://www.privacyexchange.org/japan/japanindex.html)

<sup>33</sup> These include the *Federal Trade Commission Act*, see [www.ftc.gov/ogc/stat1.htm](http://www.ftc.gov/ogc/stat1.htm); the Health Insurance Portability and Accountability Act 1996, see [www.hhs.gov/ocr/hipaa](http://www.hhs.gov/ocr/hipaa); the *Fair Credit Reporting Act*, see [www.ftc.gov/privacy/privacyinitiatives/credit.html](http://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/glbact/index.html](http://www.ftc.gov/privacy/glbact/index.html); The Can Spam Act, see [www.ftc.gov/bcp/online/edcams/spam/rules.htm](http://www.ftc.gov/bcp/online/edcams/spam/rules.htm) etc

<sup>34</sup> *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/english](http://www.kisa.or.kr/english)

<sup>35</sup> "APEC Ministers Endorse the APEC Privacy Framework", as announced by APEC Ministers in November 2004 (which also has a link to the Framework itself), online at [www.apec.org/apec/news\\_media/2004\\_media\\_releases/201104\\_apecminsendorseprivacyfrmwk.html](http://www.apec.org/apec/news_media/2004_media_releases/201104_apecminsendorseprivacyfrmwk.html). The first implementation seminar was held in Hong Kong 1-2 June 2005 and included delegates from Chinese Taipei; see [www.apec.org/apec/news\\_media/media\\_releases/130605\\_hkprivacyframework.html](http://www.apec.org/apec/news_media/media_releases/130605_hkprivacyframework.html) and [www.pco.org.hk/english/infocentre/apec\\_ecsq1\\_2.html](http://www.pco.org.hk/english/infocentre/apec_ecsq1_2.html) for a set of excellent resources.

<sup>36</sup> "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](http://www.ica-it.org/docs/issue82/issue_82_2004_04.html)

<sup>37</sup> See [www.europa.eu.int/information\\_society/europe/2005/all\\_about/benchmarking/index\\_en.htm](http://www.europa.eu.int/information_society/europe/2005/all_about/benchmarking/index_en.htm)

<sup>38</sup> The Austrian Citizen Card is described at [www.buergerkarte.at/index\\_en.html](http://www.buergerkarte.at/index_en.html)

<sup>39</sup> The New Zealand All-of-Government authentication program is online at [www.e-government.govt.nz/docs/govis2005-authentication/index.html](http://www.e-government.govt.nz/docs/govis2005-authentication/index.html)

<sup>40</sup> Excellent but lengthy papers on the PRIME project are available on the project's website, [www.prime-project.eu.org/public/prime\\_products/deliverables](http://www.prime-project.eu.org/public/prime_products/deliverables)

## Trust, Identity and Connected Government

---

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 = **Privacy and Trust**

### **Technological solutions for good identity management**

Does the technology exist to deliver good identity management, or is it just a pipe dream? The answer is clear: the technology now exists, and much of it is commercially available. A lot of work is going into developing more technologies, and more are rapidly coming over the horizon already.

It is beyond the scope of this paper to go into significant detail, other than to give some evidence that technologies that make the right claims do exist. I also emphasise that my assessment that particular technologies or commercial products can contribute to good identity management is derived from the claims made about these technologies by their proponents. For the purposes of this paper, I am taking the claims at face value. What is ultimately important, however, is that there is strong evidence that the parameters of good identity management listed in the previous section can be built into identity management systems at the technological level.

### **Biometrics without superfluous information**

A number of the biometric technologies claim that the biometric derived from the living person does not contain personal information, nor can be collected without willing cooperation nor can be used to derive the original living person's biological characteristics. For example, proponents of some iris recognition technology claim:

- “non-linkage between personal data and the template”;
- “Unlike facial recognition technologies there is no ability for the technology to capture an iris image and store it without your knowledge”; and
- “First, the iris is unable to reveal ones health, nor are revealed any predispositions to any health conditions. Secondly, there is no image of the iris stored or retrieved. Rather, a mathematical representation is stored in the IrisCode”.<sup>41</sup>

### **Multiple identifiers**

Research has already shown that it is possible to produce an infinite number of identification numbers from the one biometric source, with each of these numbers not directly linkable. This allows the one person to have a unique ID number for each application or service provider with which they interact. This research appears to have been developed in the context of iris recognition technology, but may not be limited to that particular technology. In the precise words of the researchers:

The technique described here is based on the definition of unique, application- (or even transaction-) specific formats for biometric templates that prevent the unauthorized exchange of templates across multiple applications, yet provide a mechanism for authorized transfer across applications. ...

We describe here a means for transforming a biometric template so that it assumes a new format that is unique to a particular application. Such a transformed template cannot be successfully matched to a second template extracted from the same biologic entity unless the second template is transformed so that its format is identical to that of the first template. Thus a template generated in a format corresponding to a particular application A could not be

---

<sup>41</sup> As taken from the Privacy page of the Argus Solutions website in March 2004, available at the time online at: [www.argus-solutions.com/Privacy.html](http://www.argus-solutions.com/Privacy.html).

## Trust, Identity and Connected Government

---

misappropriated and used to authenticate a user for application B because the enrolment database for application B would have a different format than those enrolled for application A.<sup>42</sup>

More recent versions of the proposed new internet protocol IPv6 are also designed to help protect online anonymity in a similar way. Through enabling users to randomise their IPv6 address periodically, and generate temporary addresses, users can prevent the creation of a unique IPv6 address that could be used to track specific users.<sup>43</sup>

A similar sort of protection is offered in the idea of 'opaque handles' in the Liberty Alliance (LA) framework for federated identity. Under a LA framework, different organisations combine to authenticate to one another the identity of an online user. LA allows (but unfortunately, from a privacy perspective, seems not to mandate) the different organisations to communicate with one another by use of "opaque handles" – unique identifiers generated purely for the purpose of exchanging data within the LA framework. This means that a person's unique identifier with organisation A is not disclosed to organisation B, and vice versa, even though A and B can exchange information reliably about that person.

### Individual control with biometrics

Biometric encryption can allow both strong encryption and provide for the encryption/decryption to be under the control of the individual, which provides further security and control. In the words of its proponent:

"I believe that Biometric Encryption provides the technological basis for informational self determination. But it requires a change in the way we think. We now have up to ten encryption keys residing at the ends of our fingers to protect our privacy and to secure information. Through this technology, security becomes a by-product of protecting an individual's privacy, and I hope you'll agree, that this is the best of both worlds."<sup>44</sup>

### Sticky privacy policies

"Sticky privacy policies" provide another privacy protective strategy within information management systems. They can be attached to individual elements of personal information, and can be enforced. Moreover, this can all be done with a very strong combination of anonymity (or at least pseudonymity). In short, such an arrangement enables an individual to exercise very fine grained control over who sees what when, and what they are to do with it. In the words of the proponents of idemix:

"[Ordinarily] the single-sign-on server knows which user accesses which service and how often. With idemix this can be prevented with only a minimal change to the overall system, i.e., only the user and the single-sign-on server need to be idemix aware. Initially, a user gets a credential for each service he or she is allowed to access. When the user wants to access a specific service, he or she only proves ownership of the relevant credential to the single-signon

---

<sup>42</sup> "Application-Specific Biometric Templates", by Michael Braithwaite, Ulf Cahn von Seelen, James Cambier, John Daugman, Randy Glass, Russ Moore, Ian Scott, *IEEE Workshop on Automatic Identification Advanced Technologies*, Tarrytown, NY, 14-15 March 2002, p.167-171, available online at: [www.cis.upenn.edu/~cahn/publications/autoid02.pdf](http://www.cis.upenn.edu/~cahn/publications/autoid02.pdf).

<sup>43</sup> See the January 2004 comments of the Electronic Privacy Information Center to the US Department of Commerce on the draft protocol at [www.epic.org/privacy/internet/IPv6\\_comments.pdf](http://www.epic.org/privacy/internet/IPv6_comments.pdf).

<sup>44</sup> "Biometrics as a Privacy-Enhancing Technology: Friend or Foe of Privacy?" by Dr. George Tomko at the Privacy Laws & Business 9<sup>th</sup> Privacy Commissioners' / Data Protection Authorities Workshop, 15 September 1998, available online at: [www.dss.state.ct.us/digital/tomko.htm](http://www.dss.state.ct.us/digital/tomko.htm).

## Trust, Identity and Connected Government

---

server. As the access is anonymous and different accesses are unlinkable, *the single-sign-on server can no longer get to know who accesses which service.*<sup>45</sup> (my emphasis).

### Technologies in combination

The combination<sup>46</sup> of such technologies outlined above with fine grained privacy specific languages such as P3P<sup>47</sup> or the next generation, EPAL,<sup>48</sup> in distributed identity systems<sup>49</sup> based on appropriate web services designs would appear to provide all the technological base that is necessary to put in place excellent security, personal control and privacy. (Indeed, the full combination as just described may have an element of redundancy built into it.)

It is clear then, that combinations of technology exist, or are being developed, with the potential to give each of us highly personal and secure control over:

- when to enrol and subsequently authenticate or participate;
- who sees what, when and what they can do with it, starting with identity authentication that of itself does not give out any more than 'bare identity'; and
- whether data sets can or cannot be 'zipped together';

while:

- authenticating identity only when appropriate (and as a consequence, allowing individuals to transact pseudonymously *and* be able conduct online many of the offline transactions that traditionally have been able to be conducted without authenticating identity);
- not being limited to one number per person; and
- not creating data trails that also become a new "honey pot" of personal behavioural information.

Because technology with all these characteristics is available, the debate over whether we need to have people identify themselves more often for a wider range of daily activities ceases to be one of capability, and becomes a matter of public policy or commercial benefit. In other words, those who wish to see society move in the direction of greater identification have to make their case without relying on arguments of impossibility.

---

<sup>45</sup> "Idemix: pseudonymity for e-transactions", available online at: [www.zurich.ibm.com/security/idemix/](http://www.zurich.ibm.com/security/idemix/). See also the slides linked from that page at: [www.zurich.ibm.com/security/idemix/idemix-slides.pdf](http://www.zurich.ibm.com/security/idemix/idemix-slides.pdf).

<sup>46</sup> See particularly "Enterprise Privacy and Federated Identity Management", presented by Dr. Michael Waidner to the [Almaden Institute Symposium on Privacy, 10 April 2003](#) and available online at: [www.almaden.ibm.com/institute/pdf/2003/MichaelWaidner.pdf](http://www.almaden.ibm.com/institute/pdf/2003/MichaelWaidner.pdf).

<sup>47</sup> Platform for Privacy Preferences, or P3P, has been developed by the World Wide Web Consortium (W3C), and "is emerging as an industry standard providing a simple, automated way for users to gain more control over the use of personal information on Web sites they visit". For more, see [www.w3.org/P3P](http://www.w3.org/P3P).

<sup>48</sup> Enterprise Privacy Authorization Language, or EPAL, has been submitted to W3C. EPAL "is a specialized language that describes and constrains the flow of personal data inside an enterprise. The tool is used to implement the paradigm of *sticky policies* ... EPAL is designed to expand on the capability of P3P by adding privacy-related access control and authorization in the enterprise context. At the same time, EPAL is a new challenge in the area of privacy enhanced technologies. While P3P was designed to be interoperable across the Web, EPAL is more focused on the intra-enterprise world." The Submission & W3C Team Comment are available online at: [www.w3.org/Submission/2003/07](http://www.w3.org/Submission/2003/07).

<sup>49</sup> For an excellent introductory critique, see "Paper – Distributed Identity – Case Studies – Parts 1 & 2: The Microsoft/IBM Web Services (WS) Security Framework and Privacy" written by Galexia Consulting in 2003 and available online at [http://consult.galexia.com/public/research/articles/research\\_articles-pa03.html](http://consult.galexia.com/public/research/articles/research_articles-pa03.html).

## **Trust, Identity and Connected Government**

---

Arguably, given the enormous economic gains (either as reduced losses through theft, fraud and national security compromises or as actual gains through improved services, aggregating to billions of dollars annually), there is also a very strong positive economic case for considering them.

The technologies illustrated here are an important start, but are not enough in themselves to ensure good identity management solutions. As with all new technologies, not everyone will trust them, systems will fail; hackers will continue in threatening data security. The future debate on how best to manage identities, however, must continue to take account of what is technically possible, and feasible.