OFFICE OF THE
FEDERAL
PRIVACY
COMMISSIONER

Proof of ID Required? Getting Identity Management Right

Australian IT Security Forum

Malcolm Crompton
Federal Privacy Commissioner

30 March 2004

Introduction[1]

Identity management and privacy: playing for high stakes

Identity management is in. It is emerging as *the* topic in government and business information technology thinking.[2]

Identity management 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[3] 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. 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.[4]

[1] I would like to thank Dr Hugh Clapin for his considerable input to the preparation of this paper. In addition, Martin O'Reilly and Christopher Jefferis provided excellent assistance.

[2] "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.

[3] The *Privacy Act 1988* distinguishes between private sector "organisations" and Commonwealth Government "agencies". For the purpose of this paper, the ordinary meaning of the term "organisation" will be used (not the Privacy Act definition), so that it means both private and public sector entities. For convenience, however, the term "government agency" will be used when referring specifically to public sector bodies, but this term will not distinguish between Commonwealth, and State or Territory, government agencies.

[4] 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.

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.

My concern is that poor identity management solutions could amount to almost total surveillance of some, if not all, individuals.

Privacy

Privacy is fundamentally about personal autonomy, and it underpins human dignity. Privacy is also integral to the fabric of society. We want to be private individuals even though we are social beings, and want to be able to interact with each other often, in circumstances where we have at least some measure of control.

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'[5] and argued for the need for a legal protection of this right in the face of 'recent inventions and business methods'.

While the world's inventions and business methods have moved on, the Warren and Brandeis formulation remains one the simplest and most meaningful answers to the question of "what is privacy?" In presenting this formulation, Warren and Brandeis have also identified the persistent challenge to privacy, posed by new technology.

Some fundamental part of human dignity requires privacy. Privacy is part of the claim to personal autonomy. It makes possible the core freedoms that democratic countries value. As then Professor Zelman Cowen said in the 1969 Boyer lectures:

> 'A man without privacy is a man without dignity; the fear that Big Brother is watching and listening threatens the freedom of the individual no less than the prison bars'.[6]

The International Covenant on Civil and Political Rights[7] is one of a number of international instruments that recognise privacy among the basic rights. Article 17 states:

> 'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.'

[5] Samuel Warren and Louis Brandeis, 1890, 'The Right to Privacy', 4 Harvard Law Review 193, 1890, and available 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'.

[6] Zelman Cowen, 1969, 'The Private Man', The Boyer Lectures, Australian Broadcasting Commission, p9-10.

[7] Accessible on the internet at www.unhchr.ch/html/menu3/b/a_ccpr.htm.

One popular analysis of privacy describes it divided into four separate but related concepts:

- 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. [8]

On another view, privacy has three elements:

- what is known about the person;
- whether there is physical access to the person; and
- whether attention is paid to the person.[9]

Despite the ordinariness of privacy, we cherish it most when we feel its absence. We notice a lack of privacy when the neighbours build a second storey that looks over the backyard. We notice a lack of privacy when a stranger unexpectedly knows about our personal affairs. We notice a lack of privacy when we find our day to day lives are under scrutiny.

The idea that privacy is a value that requires new, and stronger, protection has grown throughout the last century. Perhaps the changes to how we live in recent history have brought into focus the privacy that is being lost; whether through trends to urban living, the intrusive media interest in the famous, or the cheap availability of surveillance technology.

Privacy is not without its detractors, however. Was Sun CEO Scott McNealy right in early 1999 when he said that "you have zero privacy anyway -- get over it"?[10] Events have certainly proved that individuals, through their governments, do not want to get over it. Privacy did not die in the dotcom boom of the late 1990s. In fact, the increased use of electronic data storage and handling is one of the key drivers behind much recent privacy legislation. In Australia, for example, private sector amendments to the Commonwealth *Privacy Act 1988* were passed in 2000,[11] as was the Victorian *Information Privacy Act*.[12] In the US, it is reported that 19 separate pieces of privacy legislation were passed in 2003 alone.[13]

The two Australian privacy laws are examples of data protection laws as their focus is primarily on information privacy, or what is known about a person. Other forms of privacy, such as bodily privacy, or telecommunications privacy, also enjoy some legislative protection in various jurisdictions, for example in the telecommunications interception laws.

[8] Banisar D, 2000, Privacy and Human rights: an international survey of privacy laws and developments, Electronic Privacy Information Centre, Washington. www.privacyinternational.org/survey.

[9] Ruth Gavison "Privacy and the Limits of Law" Yale Law Journal 1980, Vol. 89 pp. 421-471 quoted in Diane Rowland, ' Anonymity, Privacy and Cyberspace' paper presented to the 15th Bileta Conference: *Electronic Datasets and Access to Legal Information* Friday 14 April 2000, University of Warwick, Coventry England available at www.bileta.ac.uk/00papers/rowland.html.

[10] "Sun on Privacy: 'Get Over It'", Wired News, 26 January 1999. Available online at: www.wired.com/news/politics/0,1283,17538,00.html.

[11] The *Privacy Amendment (Private Sector) Act 2000 (Cth).* See www.privacy.gov.au/business/index.html for more information.

[12] For more information see www.privacy.vic.gov.au.

[13] *PrivacyWeekly* 7 January 2004.

What is identity?

As we will see, identity management can be a slippery concept, in part because it is an emerging field. To investigate and understand identity management, however, we first need to understand the more basic, but perhaps more difficult, concept of identity.[14]

“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.

A person may be a corporate lawyer, a steam train enthusiast, a doting father, a lapsed Catholic, a proud migrant, an estranged son, a polio survivor, a music lover and so on. Each of those identities is valid in its own context, but personal information relevant to one identity may be inappropriate or embarrassing when taken out of context. One of the values of privacy is the ‘ability to maintain different sorts of social relationships with different people’.[15]

In addition to these relational dimensions of identity, there is also the question of self-identity. An individual’s perceptions of himself or herself include personality, degree of happiness, fears and aspirations. People need to be in an environment of trust to reveal themselves to others. An important feature of privacy is the degree to which individuals have some control over when, and to what extent, they identify themselves.

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. If we are to be carefully watched, for our behaviour to be scrutinised, it is often preferable to be anonymous. Even better, anonymity can sometimes free us from surveillance altogether.

Anonymity is sometimes thought to be an extreme method of protecting privacy. In human society, after all, it often feels unnatural to interact with others without knowing their names.

Identity and anonymity are not binary opposites, however, but different places along the same spectrum – each with many shades of grey. Anonymity is not synonymous with privacy, but is one means by which individuals can attain a degree of privacy. Anonymity can mean being unacknowledged as well as being unidentified.

[14] We have tackled this issue previously in “Under the Gaze, Privacy Identity & New Technology”, a speech to the Union Internationale des Advocats (UIA), 75th Anniversary Congress, Sydney, 28 October 2002. Available from www.privacy.gov.au/publications/index.html#S. The discussion here builds on, but owes much to, this previous paper. See also the work on identity by Roger Clarke, for example, “Authentication: A Sufficiently Rich Model to Enable e-Business” at www.anu.edu.au/people/Roger.Clarke/EC/AuthModel.html; and “Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice” at www.anu.edu.au/people/Roger.Clarke/DV/UIPP99.html.

[15] J. Rachels ‘Why Privacy is Important’ in F. Shoeman (ed.) *Philosophical Dimensions of Privacy* (Cambridge University Press: Cambridge, 1984) pp. 290-299 quoted in Helen Nissenbaum ‘Towards an Approach to Privacy in Public Challenges of Information Technology’ in *Readings in Cyberethics* by Richard A. Spinello and Herman T. Tavani (eds.) (Jones and Bartlett Publishers: Boston, 2001).

Complete anonymity is neither possible nor desirable in human society. However, a free society generally allows individuals to make appropriate choices about when, and to what extent, they reveal themselves to others. Requiring individuals to be identifiable when it is not necessary can be a form of privacy intrusion. There are circumstances where it is necessary and appropriate to ensure that a person is who they say they are. On the other hand, in some contexts, a requirement of anonymity may feel forced or uncomfortable.

In understanding identity management, it is critical to appreciate that there are degrees of anonymity. Telephone call centres recognise this when their operators provide only a first name to callers. This first name may even be fictitious, in the sense that the operator only uses it when on the phone. But it is identity enough for the job at hand. Providing just a first name – Bob from TeleHelp Inc – is much more anonymous than providing the operator's full name.

What is identity management?

> Identity management has become a hot topic among Australian corporates. … [I]dentity management projects in Australia are driven by cost and technology … lower security and administration costs are the main factors driving identity management and access management change.[16]

What could "identity management" be? I have no need to manage my own identity – I know who I am. Organisations that collect information about us, however, are increasingly seeing the need to focus on what they call identity. Why?

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.

An important issue to track down, however, is: to what extent is identity management about managing my social identity? Disturbingly, it turns out that an ill-considered approach to identity management, by not addressing these differences, could be highly intrusive, and even coercive. This paper aims to explore not only how identity management can be done poorly; but, and more importantly, how it can be done well.

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 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

[16] "Survey puts locals ahead in identity" *The Australian* 23/24 February 2004, available online at: http://australianit.news.com.au/articles/0,7204,8746813%5E15841%5E%5Enbv%5E,00.html.

- 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.

My most important goal in putting forth this paper is to open a debate on whether this is an appropriate direction in which society should head. I am not at all sure that it is, but at the same time I recognise the many valid pressures for stronger, more frequent, identity management. It is time we explored the social, economic and political consequences of identity management, in part to see if we like where it is taking us, and in part to shed light on better and worse ways to go about it.

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

Identity management, under different descriptions, has a long history, and is implemented across a wide range of circumstances. In recent times, however, it is developing a particular impetus in response to a diverse range of factors.

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 identity fraud in Australia to be $1.1bn per annum.[17] 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.[18] 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.

One kind of identity fraud that is of particular concern from a privacy perspective is identity theft or identity takeover, where identifying information about a real individual is used by someone else for criminal or dishonest ends. Victims of identity can find themselves in great difficulty, with compromised credit ratings, large debts to their name, and even criminal records recorded against them.[19] Here is one Australian example:

> In 1997, a 24 year old female applied for 61 credit cards in false names, of which 45 were granted. Some of these identities were fictitious but many of them were real, including some people known to her from her school days. This resulted in the destruction of credit of many, one of whom also suffered the additional indignity of being named by the applicant as her co-offender and mentor in the frauds.[20]

The worst instances of identity theft can result in a significant violation of privacy, in part because false and misleading information about an individual is given wide currency, and in part because of the embarrassment and discomfort in restoring one's good name.

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."[21]

Identity fraud in its various forms is not the only driver behind increased interest in identity management. Individuals recognise that there may be opportunities for increased personal convenience through better systems for establishing identity, when that is appropriate. For example, many of us would like to reduce the number of PINs and passwords we need to remember. Similarly we can see benefits in having government agencies share change of address details, so that once we have notified one agency, our details are updated with other relevant agencies.

Better identity management may also lead to improved customer service for individuals, through better customer relationship management, or through a greater degree of trust between individuals and organisations.

[17] *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.

[18] *Identity Fraud in Australia*, p. 1.

[19] For information on recovering from identity theft, and how to protect against it in the first place, see "ID Theft - A kit to prevent and respond to identity theft" published by the National Crime Prevention Program, and available from www.crimeprevention.gov.au/www/ncpHome.nsf/AllDocs/RWP41EA80A3A81A49D8CA256E1A0002A738?OpenDocument.

[20] South Australian Office of Consumer and Business Affairs, Identity Theft case studies. Available from www.ocba.sa.gov.au/consumeradvice/identitytheft/05_studies.html.

[21] 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.

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.[22]

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 Health*Connect* initiative alone is expected to achieve conservative savings of at least $300 million per annum.[23] 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. It could also improve capacity to consolidate population health data for planning and policy development by government and health providers, thus potentially improving the efficiency and effectiveness of health service delivery. Lastly, it has the potential to provide epidemiologists and medical researchers with large pools of linked data in an efficient, inclusive and accurate manner, thus contributing to clinical and public health research.[24]

The need for businesses to minimise financial losses incurred by locating debtors and settling outstanding accounts is another driver for better identity management. Commercial service providers offer services such as skip tracing whereby large databases are used to help track someone who owes an organisation money.[25]

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 – 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.

[22] See, for example, the Liberty Alliance home page at www.projectliberty.org.

[23] See Department of Health and Ageing, *Health*Connect *Interim Research Report Volume 1: Overview and Findings,* 2003, p. 9, available at www.healthconnect.gov.au/pdf_docs/cv1.pdf.

[24] For an excellent description of results already obtained in Western Australia from the Maternal and Child Health Research Data Base (MCHRDB), see the paper presented by Professor Fiona Stanley AC at the opening of the 25th International Conference of Data Protection and Privacy Commissioners in September 2003, available at: www.privacyconference2003.org/speakers.asp#fiona.

[25] See, for example, some of the services offered by commercial providers such as FCS Online (www.fcsonline.com.au) and Baycorp Advantage (www.baycorp.com.au).

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. This could be called 'go back' enrolment.

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.

One traditional method of authenticating enrolled identities is to issue the person with a card at enrolment. The production of the card, perhaps in combination with a signature or a Personal Identification Number (PIN), authenticates that the person producing the card is the same as the person who was issued the card the in the first place.

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.

In responding to these challenges, there are moves to increase the integrity of EOI documents (e.g. by making it harder to fraudulently produce or alter EOI documents, or by checking with the issuer of the EOI document that the information is valid), to increase the likelihood that the person presenting the EOI documents is the person referred to in the document (e.g. by including photographs, signatures etc. in the EOI document), and to increase the likelihood that the subsequent authentication token (e.g. the plastic card issued by the organisation) is only used by the enrolled person (again by including photographs, signatures etc.).[26]

Identity is not always the important thing to be authenticated, however.

Any sort of sale requires authentication, but not necessarily authentication of identity. In particular, the seller needs to be confident that the buyer is transferring the right monetary value, and that the transfer of value cannot be rescinded or repudiated. Cash serves this function very well, as do credit cards, debit cards, cheques etc. Cash transactions involve non-repudiable transfer of value, and require no identifying information to be transferred. Cash can be anonymous. The other means of payment, however, usually carry some form of identifying information with them, such as the person's name.

The authentication processes (e.g. comparing a signature on the card to the purchaser's signatures, having the bank authenticate the PIN of a debit card, etc.) may be best thought of as authenticating that the purchaser has the authority to use the card, rather than authenticating the purchaser's identity as such. Authorisation to enter a building can be confirmed without knowing the individual's identity. Old fashioned keys do this – simply being in possession of the key is enough to unlock a door, and thus gain entry. If keys are only in the possession of authorised persons, then possession of the key is authentication enough.

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

[26] See, e.g., "Identity fraud initiative to offer better protection for Australians". Press release by the Minister for Justice and Customs, Senator Chris Ellison, 6 July 2003. Available at www.ag.gov.au/www/justiceministerHome.nsf/0/E38F0279CAEC4CD6CA256D5B007CC6D8?OpenDocument.

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.

So while there are a lot of circumstances where something about us needs to be authenticated, it is not all that common that identity as such needs authentication.

In fact, in many situations where our identities are authenticated, what is really at stake is something other than identity. When I drive on a toll road, the toll-collector does not need to know who I am, only that I have paid my toll. When I buy goods with a credit card, the seller does not really need to know my name; only that I can transfer the correct monetary value, and that that value cannot be repudiated. A driver's licence has the core function of confirming that I am permitted to drive. For that purpose, there is no need to identify me, although this may change if I commit a traffic offence.

What if you could design a driver's licence that could only be used by the person to whom it was issued, but which carried no identifying information? Would such a device do the job of a driver's licence?

So why do drivers' licences have names and photos on them? Why do credit and debit cards have names on them? Why is there so much identification when identity is not the point at issue?

There are many reasons, the most often cited of which are national security, law enforcement and fraud prevention. If drivers' licences did not have names and photos, then, with current technology, they would be too easily transferred from licensed drivers to unlicensed drivers. If passports did not authenticate the identity of the passport holder, through name, photograph, signature etc., then they would be too easily transferred from citizens to non-citizens. And so on. Of course, identification on the face of the card also helps the licence owner know that it is their, and not someone else's, licence.

Organisations are increasingly feeling an imperative to minimise risks, whether they be risks of fraud in the financial sector, or giving someone the wrong medication in the health sector, or border security in the government sector. They assert that an obvious way to be reassured that only the right person has the key, is to connect the key to the individual's identity so that both the key, and the identity of the person using the key, can be authenticated. This is why names and photographs are on drivers' licences: to provide a link between the authorising token (the licence) and the identity of the person so authorised.

Approaches to Identity Management

There are a number of standard approaches to identity management challenges. Here are some examples.

One number per person

Much data management software relies on the use of unique identifying numbers to order individual databases. There are sound technical reasons behind this. The records which make up a database often require a key that uniquely identifies each particular record. Where the keys are numbers, it is very easy for the software to enforce the data integrity requirement that each key be unique. Whether the records happen to refer to individuals, or to widgets, the data management principle remains the same. As a consequence, large databases of personal information will invariably make use of a unique numerical identifier intended to pick out each individual.

When the issue arises of merging or linking two distinct databases of personal information, the important challenge is to make sure that, for every individual whose data is in either database, all the information about that individual is linked together. This task is made much easier if the identifier issued to each individual in the first database is exactly the same as the identifier issued to the same individual in the second database.

From the perspective of authenticating identity, if each person had a unique identifier, then authenticating identity would appear to become much easier, because the data linkages that may be involved in authenticating identity (e.g. confirming validity of a birth certificate, retrieving an electronic photograph for comparison, etc.) would be more reliable.

Inferred authentication

Carol Coye Benson suggests that an important part of the existing system of identity authentication in the US amounts to "inferred authentication". Inferred authentication includes checking an individual's claim (name, address etc.) against one or more databases.[27] Thus an organisation might look to infer authentication of my identity by collecting from me a broad range of information, then check that against a "reference" database that has been gathered together. For example, I may be asked for my name, address, previous addresses, and the kind of car I drive. This information is then submitted to a commercial data aggregator and compared against data about me that the commercial data aggregator has gleaned from a wide range of sources.

Of course, the accuracy of this method of data aggregation relies on the accuracy of the reference data. Benson argues that inferred authentication techniques are unwitting enablers of identity theft, and may themselves be violations of consumer privacy.[28]

Evidence of Identity checks

A core component of an identity management system is the way it accepts evidence of identity when an individual first "enrols" in that system. Following the *Financial Transactions Reports Act 1988 (Cth)*, the "100 points check" provides a common model.[29]

On this model, individuals may provide a range of evidence of identity, for example a birth certificate or passport as evidence of name, electoral enrolment as evidence of name and address, and so on. Different documents are accorded different values, and any combination that adds up to 100 points is considered acceptable evidence of identity.

One consequence of this sort of model of identity authentication is that it requires documents issued for a certain purpose to be used for unrelated secondary purposes. Passports, for example, are primarily issued as travel documents, not identity documents for internal, domestic purposes. As such, this model serves to embed a form of function creep into formal authentication processes.

Dangers of poor identity management

The protection of practical obscurity disappears

Identity management has been happening for a long time, for example through identifying documents such as passports and drivers' licences; through evidence of identity processes; and through access control lists in IT systems, just to name a few. In the process a lot of personal information is collected and handled by governments, businesses and individuals. Beyond identity management needs, more and more personal information is being collected electronically.

[27] Such services are offered in Australia, for example, by FCS Online (www.fcsonline.com.au) and Baycorp (www.baycorp.com.au) , although the details of these services may differ from the general description in the text.

[28] "Digital Identity: Who Wants to Know and Why?" Presentation to the 25th International Conference of Data Protection and Privacy Commissioners, Sydney, September 2003. Available at www.privacyconference2003.org/program.asp#psd.

[29] See www.austrac.gov.au/guidelines/forms/201.pdf for a standard form for the 100 point check.

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.[30] 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 who 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.

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 (for example NPP 2) that require that personal information that is collected for one purpose, not be used or disclosed for an unrelated purpose.

In the identity management arena, the use of the Tax File Number 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 1.2 of the Tax File Number Guidelines[31]), 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

[30] Information on privacy laws relevant to my Office may be found at 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.

[31] See www.privacy.gov.au/publications/tfngls.pdf.

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.

It is examples like this that drove the inclusion of NPP7 into the National Privacy Principles. NPP7 prevents private sector organisations from adopting an Australian Government identifier like the TFN or Medicare number as their own.

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 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;[32] financial affairs are recorded by financial institutions, reported to government, and held by the tax office;[33] 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

[32] 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.

[33] 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?OpenDocument. For the actual recommendations see www1.oecd.org/fatf/pdf/40Recs-2003_en.pdf. For more further information on anti money laundering reform see www.ag.gov.au/aml.

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). We are yet to feel the worst effects of this sort of data aggregation, because right now most of it is very hard to link together accurately and reliably-the "practical obscurity" protection mentioned previously. Data matching is an art,[34] and it is expensive and 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 who 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.

Given the possible public policy and commercial advantages of zipping all this data together, there is strong pressure that it will, eventually, be zipped together. It is at this point, where such privacy risks start to become reality, that individuals begin to feel that they have lost control of information about themselves. If individuals discover that organisations are linking and using information about them for purposes for which they did not consent, or start to suspect that their information can be accessed and used by persons they did not authorise, the relationship of trust is likely to start breaking down fairly quickly.

Such is the nature of identity management, that it often can be easier to be persuaded by the potential benefits of an increased collection of personal information than it is to appreciate the risks. For example, if doctors had your complete health record available, would you not receive better health treatment? If welfare agencies could know everyone's financial and employment circumstances without having to trust you to be honest, would it not save taxpayer's money? If the police had access to all the information they wanted, would it not be the case that more crimes would be solved and less crimes committed? If health researchers had access to more health records, would they not find cures and improve public health faster and more effectively? If marketers could know more about your desires and lifestyle, would not the economy, and you, benefit from better targeted marketing and advertising? If, when you changed your address with one organisation, all the other organisations you deal with automatically received the update, would this not make moving house easier? If financial institutions could better understand your financial position, could they not give you better financial advice? If a shopping centre kept a record of your physical dimensions, circulated to all the clothing shops in the centre, would this not make shopping easier? If the tax office could track every financial transaction in the country, would not everyone pay their fair share of tax? If your neighbours knew what you were thinking, surely we would all get along better?

If everyone knew everything about everyone else, would the world not be a better place?

I do not believe for a minute that anyone thinks that all of these outcomes together are desirable. We need, therefore, seriously to debate how we want identity management to proceed. There are many,

[34] 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.

with excellent reasons, who can argue forcefully for the benefits of increased data collection, and linkage, and surveillance, in some of these circumstances, considered in isolation. The most significant privacy risks are likely to arise where a number of these outcomes are justified, on narrow grounds relating to each particular circumstance, without consideration of the consequences of the combination.

Given the strong drivers behind gathering more and more knowledge of individuals – defence against terrorism; combating fraud; solving and preventing crime; protecting our borders; saving taxpayer's money; increasing sales and turnover; not to mention the potential for individuals to live more conveniently in various ways – there is very strong pressure for data that can be linked, to be linked.

This is the reason why we need to have the identity management debate now. We need to analyse objectively and weigh up all the potential benefits and risks of increased data collection and surveillance, and make a fresh assessment as to the best way to move forward so that we can ensure the best results in both areas.

However, think of some of the undesirable effects. Besides the obvious, such as the widespread circulation of your most intimate medical records, think of the more insidious. For example, think about the threat to basic democratic freedoms that could happen. The risks that are posed by increased data surveillance to an open democratic system of government have been considered by Christopher Hunter, who writes:

> Through the use of cookies, online donation forms, and political mailing lists, Internet-based campaigns can now gather tremendous amounts of information about which candidates voters prefer and where they choose to surf. The creation and sale of such detailed voter profiles raises serious questions about the future of political privacy and the democratic electoral process itself.[35]

When data surveillance expands into spheres such as this, we need to become vigilant, to prevent a slow drift towards the sort of surveillance we have seen in the past, for example that of the Stasi in East Germany.

I think it is pretty obvious that we do not want all the data that could be linked, to actually be linked together and made available willy nilly. We do not like being constantly watched and monitored by anyone, whether it be nosy neighbours, businesses, government or police. We want the freedom, at least sometimes, to experiment with new ideas, to say and do what we want, to express how we feel. As human beings we need privacy, at least sometimes.

This principle has long been recognised in the laws that regulate surveillance for law enforcement purposes. For example, to intercept a telephone call without the knowledge of the participants to the call, law enforcement officers need to demonstrate that there are reasonable grounds for suspecting that the person they are interested in is using the telephone service to be intercepted, that the interception is likely to assist in the investigation of a particular offence, and that other methods of investigation, other than telephone interception, will not be as successful.[36] In other words, the police need to have a reasonable suspicion that intercepting these particular phone calls will assist them in investigating a specific crime, and they have to get permission to do so in a way that also costs time and money, for example taking out a court issued warrant. As a society, we recognise the need to balance the value to law enforcement of surveillance with the risk of treating everyone, all the time, as a suspect.

[35] "Political Privacy and Online Politics: How E-Campaigning Threatens Voter Privacy". *First Monday,* volume 7, number 2 (February 2002), url: http://firstmonday.org/issues/issue7_2/hunter/index.html.

[36] See, e.g. s. 45 of the *Telecommunications (Interception) Act 1979* (Cth).

Identity Management, data linkage and surveillance

What is the connection between identity management and the worst-case scenario of total surveillance?

For example, one common tool in identity management is the photograph. Comparing the photograph on a card to the individual presenting the card is, in many situations, a reasonably good way of authenticating the identity of that person. Facial recognition technology is increasingly able to do this comparison automatically. Apparently, under the right conditions, the technology is becoming reliable in comparing a live face to a database record of a face, and confirming that the two match.[37] In fact, some computer facial recognition is arguably better than that done by people.[38] It is likely that in the future facial recognition technology may become able to compare a photograph against a big database of other photographs, and detect a match.[39] Conceivably, this technology could even take surveillance camera or other video footage and identify the individuals in the video.

Photographs used to be reasonably difficult to reproduce and impossible to compare without human intervention. Digitised photographs are easy to copy and disseminate, and increasingly can be used in computerised data matching.

The consequence is that, if the facial recognition software were to be perfected, every database of information containing a digital photograph could be reliably linked. The digital photo becomes the linkage key by which masses of unrelated data can be linked, and, ultimately, each of us can be tracked.

This illustrates the most important danger of poor identity management: the identifiers that reliably link the data to the person, also reliably link unrelated sets of data to each other. Increased data linkage in a world of increasing data collection leads to comprehensive surveillance.

Good Identity Management

Bad identity management involves collecting and handling as much identifying data as possible in order to be confident at every step, from enrolment to subsequent transaction, to interlinkage with other organisations or data collections, that the organisation is dealing with the right person, whether or not the person's identity is the relevant issue.

What, then, is good identity management?

Good identity management involves processes that meet the same goals – 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. Similarly, where I describe particular technologies, or commercial products, in the context of good identity management solutions, or privacy enhancing technologies, I am endorsing only the potential of the technology or product, or general approach, to contribute to an overall solution that is

[37] See, for example, information from the Australian Customs Service about an evaluation of the trial of the SmartGate face recognition system (available online at www.customs.gov.au/resources/Files/media%20background%20smartgate.pdf).

[38] See, e.g. "Researcher faced with identity crisis" *The Australian* Higher Education section, 17 March 2003.

[39] See, for example, the following Face Recognition Vendor Test, available on the Biometrics Institute website, which tested scenarios such as verification, identification and comparison against a watch list: www.biometricsinstitute.org/bi/FaceRecognitionVendorTest2002.pdf.

privacy enhancing. Almost any of the specific commercial products mentioned in the next section ("Technological solutions to good identity management"), for example, could be implemented in privacy invasive way, or form part of an identity management solution that, in the end, failed to pass the privacy test.

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. I may be known as "Malcolm" to the waiter in the local café, but "The Commissioner" to someone else. Many people change their name through marriage or divorce, creating distinct groups of people who know them by one name but not the other. An immigrant from a non-English speaking background may have an anglicised name as well as the name she is known by in her community. A common reason for a change of name among some Indigenous Australians is that a person with the same name has passed away, and that name can no longer be used.[40] Online environments often allow individuals to choose freely the name by which they will be known in a particular 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 us 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

[40] For more information on privacy and Indigenous Australians, see *Minding Our Own Business*, available on the web at www.privacy.gov.au/publications/index.html#M.

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.

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 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.

Another mechanism that facilitates the use of multiple identifiers across different systems, while allowing those identities to be linked under appropriate circumstances, is offered through the client master index approach used by some health records managers. Individuals are often issued with different patient identity numbers at different health facilities. A client master index is a list which matches these identity numbers together, so that my public hospital identity number can be matched to my private hospital identity number, and so on. Client master indexes present strong privacy risks, of course, because they are precisely designed to match data from different data silos. Where such data matching may be appropriate (for example, where it takes place under the control of the individual concerned), then the value of a client master index approach can be that it keeps the data separate, and retains the separate identities associated with the different health care providers, while facilitating the combination of health information only where this is appropriate.

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 my 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 makes biometric identifiers attractive is that they are precisely 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.[41]

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 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.

[41] See “Fingerprint Fear”, New Scientist, 2 May 2001, at 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.

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 gelatin, defeated 11 different commercial fingerprint readers [42]

Data silos

Remembering that data linkage is the 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.

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.[43]

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.[44]

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;

[42] See: "Jelly babies dupe fingerprint security", ZDNet, 17 May 2002, at www.zdnet.com.au/newstech/security/story/0,2000024985,20265318,00.htm.

[43] 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.

[44] "IBM Scientists Rely on the Principle of Uncertainty To Develop Web-Privacy Answers", IBM Press Release of 23 May 2002, available online at: www-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.

- 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.

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”.[45]

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. …

[45] As taken from the Privacy page of the Argus Solutions website, available online at: www.argus-solutions.com/Privacy.html.

> 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 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.[46]

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.[47]

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."[48]

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

[46] "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.

[47] 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.

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

> 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 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*."[49] (my emphasis).

Technologies in combination

The combination[50] of such technologies outlined above with fine grained privacy specific languages such as P3P[51] or the next generation, EPAL,[52] in distributed identity systems[53] 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.

[49] "Idemix: pseudonymity for e-transactions", available online at: www.zurich.ibm.com/security/idemix/. See also the slides linked from that page at: www.zurich.ibm.com/security/idemix/idemix-slides.pdf.

[50] 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.

[51] 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.

[52] 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.

[53] 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.

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 it manage identities, however, must continue to take account of what is technically possible, and feasible.

Achieving good identity management

What does success feel like?

Identity management can seem very different, depending on the context in which we experience it.

As individuals we can feel the increasing demands to prove who we are to be intrusive, embarrassing, or inconvenient. As individuals, we can also feel reassured that the organisations are making sure that someone else is not able to pose as us.

Organisations see identity management in terms of the business goals it will assist, key amongst which are probably risk management goals. They ask themselves how exposed is the organisation to fraud of various sorts? What steps can be taken to minimise financial or other losses, and to minimise culpability if something goes wrong?

Governments see identity management in terms of their key responsibilities, such as providing a safe and secure society, efficiencies, and resource accountability.

As the Federal Privacy Commissioner, I see identity management as a high stakes project requiring very careful handling.

What, then does, successful identity management feel like? How will we know when we have got it right?

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 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 are having 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.[54]

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 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 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 organisations. 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 obligations 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 the 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

[54] For example, in a survey on community attitudes to privacy conducted by my Office, it was 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, July 2001. Available online at www.privacy.gov.au/publications/rcommunity.html#4.31.3. 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", January 28, 1999, available online at www.chcf.org/press/view.cfm?itemID=12267.

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 questions 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 different 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.

Organisations can also measure their identity management systems in terms of efficient data management. An identity management system that collects more information than required, and collects it in a form that is easily linkable to other data, will find itself with increased data security risks and greater data management headaches. If important identity information, and authentication of identity information, is collected and stored, then that data will be a valuable commodity that needs to be protected. A high integrity database of, say, names, addresses, passport numbers, driver licence numbers, digital photographs, and digital fingerprints, all stored in an easily usable form, would be a significant target, as it would provide an excellent source for identity theft, to name just one example. The collection of too much data, arising from excessive identity management solutions, thus can create unnecessary data management headaches.

The right approach

I hope to have clearly shown the privacy dangers posed by certain approaches to identity management. The dangers, however, extend well beyond the lives of the individuals whose privacy is adversely affected. There is significant potential for the wrong sorts of identity management solution, or the wrong implementations of identity management in large scale contexts, to have a detrimental impact on the trust of individuals in governments and businesses.

I have also been able to illustrate that the challenges of identity management can be met while protecting privacy and consolidating, or even increasing, the trust that is an essential part of our social fabric.

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.

In response to recent pressures on Government to investigate new law enforcement and security powers, my Office developed 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.[55]

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.[56]

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 everpresent, 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 regulation (for convenience, I will refer to these kinds of structures as “law”.). It is the nature of such promises, however, that the 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.[57]

[55] 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) 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).

[56] 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 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. The Office is also currently working on a draft of a more detailed document, which is intended to offer further advice on what matters an agency or organisation might consider when conducting a Privacy Impact Assessment. We will be consulting on the content of this draft, and hope to release the paper in the near future.

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. The technological solutions to good identity management we discussed previously provide good examples of how the technology offers an important part of a privacy-enhancing solution to good identity management.

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 (as provided by my Office under the Privacy Act, for example), such transparency contributes to an accountable system.

It is the overall combination of legal and policy frameworks, delivered through privacy-enhancing technology, under a transparent and accountable system, the 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 though law, standards, or other policy commitments, and adherence to these parameters is ensured through appropriate mechanisms of transparency and accountability.

The identity management debate

As we have seen, the drivers behind increased and improved identity management can be powerful and important. As Federal Privacy Commissioner, I can not ignore the valid pressures for appropriate identity management. But nor can I, or should I, accept that privacy will be sacrificed along the way.

A widespread implementation of simple-minded identity management solutions is likely to result not only in a massive loss of privacy, but also significant change for the worse to the nature of society and how we live in it.

Such an outcome is entirely unnecessary, and now is the time to focus our attention on the good solutions to identity management. I have advocated here a framework for ensuring we can manage our identities so that we have a safe, secure and open society, where we all do have a private life.

The framework starts with applying the AAAA Framework of Analysis, Authority, Accountability, and Appraisal, throughout the information 'life cycle'.

This framework will deliver if:

Law + Technology + Market + Transparency + Accountability = Privacy

Finally, from within this, good identity management will produce results where:

[57] 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.

- 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.

I recognise that at times privacy will be adversely affected through necessary identity management initiatives. Where this has to happen, however, it will be as a last resort where the opportunities for good identity management solutions have all been exhausted.

The practical consequence, then, is that there will be, and needs to be, ongoing debate about when new identity management solutions are necessary and what those solutions should be. I have presented one view of good identity management. I am sure this is not the only view. We need, most of all, to make sure we continue an identity management debate that is well-informed and constructive.

After all, privacy is a fundamental human right.