Who am I ?

Dispelling the annoyingly persistent myth of a single answer

Nigel Waters[1]

A Paper for [Id]entity 08 – a conference organised by the Office of the Victorian Privacy Commissioner, Melbourne, 12 November 2008

> “In existentialism, the individual's starting point is characterized by what has been called "*the existential attitude*", or a sense of disorientation and confusion in the face of an apparently meaningless or absurd world.”[2]

Who are these people?

Charlotte Eugenie Smith - Charlie at school – grown out of it but still used by relatives and close friends - hates Eugenie and never includes 'other/middle names' fields on forms. Marries Juan Spaniolo, but continues to use Charlotte Smith in her professional life and has bank accounts and investments in that name (without Eugenie or E) as well as new joint accounts as Mr & Mrs Spaniolo. On-line, uses Charles Smith to minimise objectionable email.

Mary Hoa – an orphaned refugee from Vietnam in 1974, born (she was told) and registered on arrival as Duong Thi Hoa, DoB 21 June 1963. Her name is regularly recorded in incorrect order (would you know?) - has been known as 'Mary' since being fostered and now finds it convenient. Recently discovered evidence of her true birth date as 21 October 1962 and changed it with the Registrar, but many existing records still have her old 'presumed' DoB.

Piotr Wrackmanski - registered by his father as Peter Rackman on arrival in Australia as a toddler. Ironically known to his workmates and family as 'Pole', which he is happy to use instead of Peter in many ordinary transactions – but when filling out official forms he is often uncertain whether to put Piotr W or Peter R.   Has had some mental health problems for which he has chosen to receive private psychiatric treatment using the name Peter Warne.

Simon Townsend – born Michael Warwick, 24 May 1963, London, but relocated to Sydney in 1994 as a protected witness and given a new 'official' identity of Simon Townsend, born 12 July 1964 in Manchester. Simon/Michael's wife and three children also have new identities as the Townsend family, although he is fearful that some of them may have remained in touch with some of their old friends and thinks that the children may want to re-assert their birth identity once they become independent. 'Michael' stands to inherit a substantial sum from his uncle and still owns a house in England registered in that name.

[1] Nigel Waters is Principal of Pacific Privacy Consulting, a Board member of the Australian Privacy Foundation and a member of the Executive of the Consumers Federation of Australia

[2] Robert C. Solomon, *Existentialism* (McGraw-Hill, 1974, pages 1-2) (via Wikipedia)

The myth of a single identity

Some people, and most organisations, unconsciously assume that each human being is tied to a single 'true' identity, and anything else, any other identity for that person, is a mistake, dishonest, or even illegal. This is understandable, but plain wrong. This false myth has serious adverse consequences that we should understand and fix.

The reality is that thousands of people, like the four exemplars above, have more than one 'label' by which they are known in different contexts – in effect different identities.

To the extent that addresses are used as a component of evidence of identity (EOI – never POI!), often as a tie-breaker for the surprisingly large number of individuals with the same name and birthday, the permutations and complexities are multiplied – as many individuals have more than one legitimate address: - e.g. residential, postal, holiday homes, city apartments.

Many government agencies and private sector organisations appear to think that everyone has a single 'official' identity, with all other 'labels' being aliases, 'known as...' or 'other names'. Similarly, individuals are expected to have one 'primary' address, even if that is not the way they live.

No legal basis?

As far as I have been able to establish over many years, there is no legal basis for these assumptions. Many laws require individuals, when giving their 'name' or address in a particular context to use a particular specifications, but these requirements are not all consistent. In many circumstances, it is perfectly legitimate to use a name that you are 'commonly known by' provided there is no fraudulent intent, and to give any valid address.

Underlying lack of trust

This goes to the heart of the issue – many of those seeking to attribute a single official identity to us appear to be doing on the basis that the general public can't be trusted not to use different 'labels' to avoid obligations or carry out unlawful acts. Clearly many people will use labels in this way - perhaps a growing number, although I have seen no hard evidence of that. But does that justify treating everyone as though they have this intent?

Surely the answer to that question depends on a number of factors:

- The 'risk' to society of allowing individuals to use alternative labels, which in turn is a function of both *frequency* of abuse and the *extent* of any harm that can result. Empirical evidence of the extent of identity crime is notoriously elusive and questionable.
- The alternative means available to deter, detect and remedy any abuse – such as more resources for investigation and heavy penalties for use of alternate labels for evading obligations or other fraudulent intent. What is the evidence that these more traditional approaches to compliance enforcement cannot be both effective and efficient?
- The risks both to society and to individuals of enforcing a 'single official identity' policy – for instance in increasing both opportunities for and consequences of identity crime by third parties, or in making it harder for individuals to protect themselves – e.g. from abusive partners or unstable clients.
- The residual risk of identity crime *even after* enforcement of strict 'single identity' policies, and the potentially greater impact of this in an environment where most users perceive the 'official' system as more reliable. Even in the most autocratic societies, there is a thriving market in false identities, and technology will never provide a complete answer.
- The value we place on individual freedom and autonomy. Provided I am prepared to

> disclose any other relevant labels in specific contexts, what right has the State, let alone any private sector organisation, to determine how I present myself?

Managing complexity

We can all fully understand the desire of bureaucrats (both public and private) to try to 'order the world' for administrative convenience and least cost. Any of us who have struggled to keep a simple mailing list up to date and accurate can sympathise!

But surely the mantra of 'risk management' should be applied to identity management, instead of a futile pursuit of risk elimination, which is doomed to failure.

And shouldn't we be clever enough to be able to manage complexity, rather than crudely trying to hammer 'rounded' individuals into square holes?   There are plenty of imaginative ideas around for doing so in relation to identity management – such as the many examples of federated or distributed identity systems, where identity is specified and managed in relation to a particular functional need, with links and associations made and stored only as and when required. The resources listed at the end of this paper provide links to some of the discussion around these approaches

Unfortunately, these solutions still generally languish in the academic and NGO communities, and the mainstream government and private sector identity management initiatives still appear to be determined to pursue simplistic 'single identity' approaches, despite all the evidence that this is a unachievable goal.

Associated concerns

Attempts at 'unique' labelling, often involving the assignment of an identifying code or number, cannot be divorced from their intended uses, and opposition to such schemes is as much to do with concerns about centralised databases, data sharing and matching and 'function creep' as it is objection to the ID scheme itself.

In fact it is these other pressures that are creating the real problem – few of us have any difficulty with the use of 'purpose specific' identification numbers or codes such as TFNs or Medicare numbers – they are sensible ways of managing the complexity of names and other identifying particulars. Nor is there any 'in-principle' objection to law enforcement agencies being able to link separate identities when justified for specific investigations – subject of course to appropriate controls and oversight.

It is when governments try either to use existing identifiers in ways for which they were not designed, or to create new 'multi-function' identifiers, that they come up against both practical limits and philosophical and moral objections.

In Australia, we have seen attempts to impose a national identification scheme defeated twice in the last 25 years – most recently with the demise of the last federal government's proposed 'Access Card'. The dishonesty with which the scheme was 'sold' and the failure to admit its real nature probably contributed to its demise. But so too did a deep-seated objection by many Australians to being centrally and uniquely registered and labelled for the convenience of government, betraying a fundamental lack of trust.

Proposals for much needed electronic health records (EHR) also continue to founder partly because of the refusal of their proponents to address legitimate concerns about centralisation of sensitive data and the role of unique identifiers. Federated or distributed models of identity management offer a way of breaking this deadlock, yet health bureaucrats continue to resist anything other than a overall 'big bang' solution.

Technology suppliers lobby aggressively, but short-sightedly, in support of centralised databases and identifiers, despite the fact that there are probably greater commercial opportunities, long term, in federated or distributed systems.

Overall, a failure of imagination and refusal to think past traditional 'managerialist' models leaves us stuck in a quagmire – unable to reap the many obvious benefits of information systems unless legitimate privacy and security concerns are addressed, but unwilling to apply our collective intelligence to managing complexity rather than pursuing a holy grail of simplicity and order.

Identity Management in Australia

Currently in Australia, there are many identity management initiatives under way, at both the Federal and State and Territory levels, and increasingly in joint inter-governmental projects, and/or partnerships involving the private sector. They include:

- A National Identity Security Strategy, comprising work on:
  - a Standard framework for Proof of Identity (POI) and Enrolment Processes
  - Security Standards on POI documents
  - a Document Verification Service
  - the Integrity of Identity Data, and
  - Authentication standards.
- Electronic Verification for AML-CTF Act purposes.
- ALRC proposals for more comprehensive consumer credit reporting
- Various 'single sign-on' and authentication initiatives for access to government services.
- Various employee ID initiatives including for airport and port security, and for the Australian Defence Forces.
- Increasing cooperation between Registrars of Births, Deaths and Marriages.
- Driver licensing authorities moving into identity verification roles.
- Ever-increasing secondary uses of Electoral Rolls.

Some of these initiatives are, belatedly, recognising privacy issues, with the growing use of Privacy Impact Assessment techniques, although depressingly few of the initiatives are as transparent as they need to be, with limited opportunities for public consultation and debate.

What is still completely lacking is an overall national debate about the appropriate limits of identity management, and in particular the merits of functionally limited schemes and federated solutions as an alternative to universal unique identifiers and centralised databases. The recent ALRC Report[3] touches on the issues – including in chapters on Definitions; Identity Theft; the Identifier principle and Credit Reporting – but does not do them full justice.

Leadership required

Privacy Commissioners should be leading this debate, as they are starting to do in Canada and Europe. This conference is a welcome initative by the Victorian Commissioner, and a good start, but is no substitute for a wider national discussion.

[3] ALRC Report 108, *For Your Information: Australian Privacy Law and Practice*, May 2008

Privacy and consumer advocates are willing, and indeed eager, to participate in this discussion (to the extent that their limited resources allow – engagement with civil society has a cost which needs to be included in the budget for these initiatives).

Governments need to create the opportunities for a free, open and thorough discussion of identity management – otherwise they will repeat the mistakes of the past with millions of dollars wasted on over-ambitious IT projects that founder on the rocks of consumer suspicions and mistrust (amongst other hazards!).

An integral part of the debate must be an acknowledgement there may often be no simple answer to the question 'Who am I?'.

Resources

On the Identity Trail – a joint project involving the Information and Privacy Commissioner of Ontario and various North American Universities and NGOs
http://www.idtrail.org/

The Identity Project at the London School of Economics
http://identityproject.lse.ac.uk/

David Lyon and Colin Bennett (2008) Playing the Identity Card: Surveillance, Security and Identification in Global Perspective, and more generally The Surveillance Project at Queens University, Canada http://www.surveillanceproject.org/

John Harrison and Pete Bramhall (2007) New approaches to identity management and privacy: A guide prepared for the Information Commissioner

Roger Clarke (2004) Identification and Authentication Fundamentals and many other papers at http://www.anu.edu.au/people/Roger.Clarke/DV/AnnBibl.html

Galexia Consulting (2003) Distributed Identity Case Studies and other relevant papers at http://www.galexia.com/

... and for a fun but highly relevant presentation by Dick Hardt - Identity 2.0

Contact: Nigel Waters Tel: 02 4981 0828 Mobile: 0407 230342	Australian Privacy Foundation http://www.privacy.org.au
Pacific Privacy Consulting www.pacificprivacy.com.au nigelwaters@pacificprivacy.com.au	Consumers Federation of Australia http://www.consumersfederation.org.au/