Introduction

This paper examines the question: How can privacy risks be understood and managed within large-scale identity management systems?

We argue that new forms of identity management – in the form of distributed identity – can address and manage privacy protection within their technical design. Such systems, backed up by effective Privacy Management Strategies, can restore trust and confidence in identity management systems amongst the wider community. Distributed identity schemes are identification and authentication systems which may operate as alternatives to centralised, ‘single database’ identification schemes. They include the concepts of federated identity and identity broking.

Distributed identity is being considered as a privacy positive alternative to centralised identification schemes. This paper argues that while distributed identity may be a reasonable alternative to centralised identification schemes, distributed identity is not necessarily a privacy positive initiative unless it is implemented in a certain way. The level of privacy intrusion depends on numerous technical factors and the effective management of privacy issues during design, implementation and the active life of distributed identity systems.

We conclude that both federated identity and brokered identity models have something to offer, and recommend that distributed identity models are most likely to deliver privacy-friendly identity management in the Australian context.
Identity management

The two core approaches to identity management are centralised systems (such as national identity cards) and distributed identity systems (such as federated identity and brokered identity). Distributed identity is being considered as a privacy positive alternative to national identification schemes, such as the failed Australia Card proposal (Clarke 1987) and the failed proposal to merge government databases in Ontario, Canada.

Trends and drivers in identity management

The need for identity management systems, including distributed identity solutions, is being driven by several trends. The motivation for the wider acceptance and use of these systems comes from a variety of sources within both the public and the private sector.

Government trends

The uptake of e-government will involve, as a key prerequisite, coordination and facilitation of the development of a trusted and secure online environment for delivery of government services, to both individuals and businesses. However, government agencies appear to remain uncertain of the availability, cost-effectiveness and inter-operability of technologies, tools and standards for identifying and authenticating online customers. Consequently, this is holding back the rollout of more complex or sensitive e-government services and transactions, thereby delaying more widespread benefits of e-government.

Electronic authentication is qualitatively different for the public versus the private sector because of government’s unique relationship with citizens:

a. many of the transactions are mandatory
b. agencies cannot choose to serve only selected market segments
c. relationships between government and citizens are sometimes ‘cradle to grave’, but characterised by intermittent contacts, which creates challenges for technical authentication solutions
d. individuals may have higher expectations for government agencies than for other organisations with regard to protecting the security and privacy of personal data (The National Academies 2003, Section 6.2).

In Australia, federal government agencies are working with the National Office for the Information Economy to develop an identification and authentication framework which can accommodate various agencies’ business processes while providing common standards and rules (National Office for the Information Economy 2003). There is also a strong international interest in e-government initiatives (Accenture 2003).

Business trends

Businesses are investigating the use of identity management systems to provide services more efficiently. Costs can be reduced by sharing authentication and verification credentials across a wider range of organisations – rather than creating stand-alone authentication systems for each organisation and/or application. Identity management systems may enable multiple-subsidiary e-business transactions to be streamlined and simplified.
Key issues in identity management

Identity management systems do not exist in a policy vacuum. The context and setting for identity management solutions should have a direct impact on design and implementation; addressing these key issues at the design stage of identity management systems has significant benefits over attempting to manage these issues post-implementation. Management of these issues in distributed identity models is essential, and it should not be assumed that distributed identity models will ‘automatically’ be more effective at addressing these issues than centralised identity models.

Models fore-authentication

The strength of the authentication method employed in any system should be commensurate with the value of the resources (information or material) being protected (The National Academies 2003, Recommendations 2.1. & 4.1).

Evidence of identity

Sufficient levels of trust and confidence must be generated in the accuracy and validity of information which is presented as original evidence of identity.

Many of the foundational identification documents used to establish individual user identity are very poor from a security perspective, often as a result of being generated by a diverse set of issuers that may also lack an ongoing interest in ensuring the document’s validity and reliability (The National Academies 2003, Section 6.3).

Data retention

Sufficient records must be retained to assist in future investigations or inquiries. The validity and accuracy of such records must be balanced against privacy interests.

Privacy

Appropriate privacy controls must be provided within the solution, including the ability to provide anonymity where necessary. Privacy controls need to go beyond simple compliance with national and international privacy laws. They also need to meet the privacy expectations of consumers.

Identity fraud and identity theft

Identity management systems need to limit opportunities for common identity fraud (one-off fraud which usually relies on the adoption of another person’s identity for a single transaction) and provide adequate prevention against identity theft (more sophisticated fraud where a false identity is assumed for opening accounts, obtaining multiple goods and services etc.).

Legal liability

Identity and authentication system users also wish to ensure they are properly protected by the law. Allocation of legal liability for unauthorised transactions must be determined for each solution.

Distributed identity

Although distributed identity may be a reasonable alternative to centralised schemes, distributed identity is not necessarily a privacy positive initiative in its own right. The level of privacy intrusion depends on numerous technical factors and the effective management of privacy issues during design, implementation and the active life of distributed identity systems.
Distributed identity involves exchange of identity information across one or more trusted domains (either within a single organisation or between different organisations) in such a way that the information is maintained at its original source.\(^1\)

To manage authentication and verification, distributed identity systems may use either a ‘web of trust’ (federated identity), or a ‘trusted third party’ (brokered identity).

Where it is necessary for users to gain access to multiple applications provided by multiple organisations, distributed identity allows single sign-on by passing through user authentication and authorisation credentials.

In a recent document, looking at federated network systems, such a network is described as: ‘A networked world in which individuals and businesses can more easily interact with one another, while respecting the privacy and security of shared identity information’ (Pato & Rouault 2003, p. 5).

Often, a common feature of distributed identity systems is that users are provided with an opportunity to exercise some control over the type and amount of information disclosed to different organisations for different applications.

**Federated identity**

Federated identity is a type of distributed identity which relies on communities of trust. Examples of federated identity models include Liberty Alliance,\(^2\) WS-Federation,\(^3\) and smaller sectoral initiatives.

The concept of federated identity is that personal information remains in the hands of the original collector and is shared across a wide range of providers, instead of consolidated into a master database. The relationships between providers are regulated by private contract and applicable privacy and data protection laws.

**Liberty Alliance**

Liberty Alliance is an open technical specification for sharing personal information through computer networks like the Internet. It is highly sophisticated and mainly useful to very large corporations and government organisations that conduct transactions online.

Liberty includes several technical privacy features in its specifications, such as anonymity option, and consent markers. However, as a standards body, it cannot enforce many policy aspects of privacy on its users.

The broad usage of Liberty in retail e-commerce seems some time away, given consumer resistance (Wicox 2002) and the expense of deployment. The more viable – and less privacy intrusive – applications are for more discrete networks of users and providers, rather than large-scale business-to-consumer applications. For example:

- **Financial trading communities** – a relatively small set of users who would benefit from consistent access to a variety of disparate market systems. The privacy implications are limited given that only limited personal information is needed, and the usability benefits are significant.

- **Student and employee intranets** – large companies, universities and other education institutions often have a number of separate internal information technology systems. Here the incentives for identity fraud, or privacy abuse by the controller, are low, and the benefits once again are significant (in Australia, however, it is important to note the legal vacuum relating to employee privacy).
• **E-government** – although the risks of identity fraud are significant, governments are generally subject to a degree of privacy regulation and oversight, and the efficiency and cost savings from achieving interoperability between various government applications provide a genuine incentive to governments to be some of the first adopters of Liberty technology.

However, it is large consumer corporations – credit card companies, technology vendors and private telecommunications providers – who are currently considering the future benefits of Liberty, and backing the Liberty Alliance:

Deploying [single sign-on] functionality will drive additional requirements for attribute sharing in order for banks, insurance companies, brokers or others in the industry to deliver more personalized services to their users. Liberty’s first set of specifications and future work is playing an important role in this area (Liberty Alliance 2003).

This vision of seamless web services for consumers is not so comforting to privacy advocates. Despite the protests to the contrary by Liberty Alliance backers, the fact is that wide deployments of any particular standard in online authentication and information sharing can raise potential privacy risks.

Given that Liberty is a draft technical standard, and does not have any enforceable control over implementation, consumers will have to rely on existing privacy regulatory schemes and trust corporations to run their Liberty-enabled systems responsibly.

Liberty Alliance must now take further responsibility for providing comprehensive guidelines and promoting good privacy among its members. Its online tools will need to be supported by enforceable customer-protective policies and practices (of the organisations using those tools), for Liberty to be seen as offering a privacy-sensitive identity management solution. The success of Liberty’s concept of ‘federated network identity’ rests on its ability to ensure information sharing does not run rampant over the interests of consumers.

**WS-Federation**

In April 2002, IBM and Microsoft jointly published the white paper *Security in a Web Services World* (IBM & Microsoft 2002), dubbed the ‘roadmap’ of a secure web services framework, together with its founding WS-Security specification. The roadmap sets out a body of protocols that would use XML messages as a standard way for computers to communicate service requests to each other, regardless of the software or hardware they used – the web services model. Several of those protocols have now been published, forming the WS framework.

For now, the WS framework provides an advanced security infrastructure for integrating enterprise information technology systems. Eventually it aims to provide security and services for distributed applications for both consumers and businesses.

WS is, at best, a skeleton distributed identity system. The nature and content of the information exchanged is not dealt with by the WS specifications. Only WS-Federation and WS-Privacy really contemplate the identity federation applications of the WS system. But WS provides a highly advanced ‘infrastructure’ necessary for such information exchange.

WS-Federation brings together other WS standards to describe a ‘federated’ web services model, and details the use of identifiers and pseudonyms across service providers and requestors. It also considers the types of transactions that could occur and some of the privacy and security precautions applied to a federated system.
WS-Privacy is not yet published but it is described in the roadmap document. It may use other WS specifications such as WS-Security (for basic security), WS-Policy (as a structured way to ask privacy questions) and WS-Trust (as a way to manage privacy across several transactions) to provide for privacy controls in web services networks. Systems can use WS-Privacy to make assertions about their privacy practices – for example, they can promise not to pass the data on to any third parties.

The next release of Microsoft Windows will incorporate the WS framework. However, for the immediate future, WS is faced with the classical paradox of distributed computing open standards; they only become useful when everyone has them. Accentuating this paradox for IBM and Microsoft is the fact that the WS project is more abstract than other sector initiatives like Liberty Alliance or the original Microsoft Passport concept. Instead of concentrating solely on identity management, the WS framework is designed to enable more general types of transactions.

At the time of publishing, prior to the release of WS-Privacy, the WS framework provides a small number of privacy features in addition to its security basis. WS-Federation allows for the optional use of ‘opaque identifiers’ so that no identifying information need be shared for basic identity federation functions.

The WS-Privacy concept is an encouraging step towards making privacy a functional part of information technology systems. But implementations of the specification will not do any better at protecting privacy than they are designed to. WS-Privacy may provide a useful tool for enforcing the rules but good privacy, just like good business, is based on treating customers fairly and with respect, not just complying with the legislation, as may be the temptation with a WS-Privacy system.

**Brokered identity**

Brokered identity is a form of distributed identity management which relies on the services of a trusted third party to manage authentication and identity on behalf of consumers.

Reach is an example of brokered identity. Reach is an agency established by the Irish Government in 1999 to develop a strategy for integrating public services and to develop and implement a framework for e-government. In May 2000 the Irish Government commissioned Reach to develop the Public Services Broker. Since then, Reach has focused on defining and implementing the architecture and principles underlying the operation of the Public Services Broker (Department of Social and Family Affairs 2002).

Reach’s mission statement is:

> to radically improve the quality of service to personal and business customers of Government and to develop and deploy the Public Services Broker to help agencies achieve that improvement. In particular Reach is to develop and implement an integrated set of processes, systems and procedures to provide a standard means of access to public services, to be known as the Public Services Broker.

This electronic broker will act as a helper or assistant between customers and Public Service agencies. It will be developed by Reach and then subsequently be operated by a separate agency. The Public Services Broker is not intended to act as a representative or advocate for government agencies.

As part of its work with the Public Services Broker, the Reach project is developing standards and legislation that will deal with issues of interoperability, Internet security and privacy. Reach aims to provide a one-stop service for public service customers; enabling them to access related services at a single point of contact and to give their information, and prove their identity, once only, instead of having to go through the same procedure separately for each related service. To improve services in this way, internal business processes need to be integrated. Data-sharing is a key to facilitating the seamless
delivery of public services – it promotes customer service and efficiency and reduces the need to call for physical documents.

However, there is also the requirement of meeting customers’ expectations that data is kept securely and that their privacy is respected. In response to this, the Reach model seeks to balance the need for the availability of data to public service agencies while ensuring a high level of privacy and respect for data protection principles.

Reach is implemented as an element of the Irish Government’s broader e-government strategy which aims to ensure quality of service to people dealing with government agencies and improvements in administrative efficiencies. \(^{11}\) Reach is also responsible for ensuring the development of electronic government in Ireland is done in the context of European Union initiatives. This involves complying with the eEurope Action Plan (Commission of the European Communities 2002) which sets the e-government strategy in the wider European context and places certain e-government development obligations on Ireland.

The Public Services Broker is the central component of Ireland’s e-government strategy. It provides a common access point for e-government services, identity management and access control, common interface standards, procedures and supporting services with the necessary infrastructure to make access to e-government services as straightforward and secure as possible. \(^{12}\) The Public Services Broker aims to improve delivery of services to the public through traditional means (in person and on the telephone) and the new self-service electronic channel (Irish Internet Association 2002).

The Public Services Broker model involves an integrated approach on three levels:

- a single access point to related services (integration across agencies, services and transactions)
- updated data available in real-time and data available for repeat transactions (integration across time)
- the same data and experience available across the three main access channels – counter, telephone and the Internet (integration across channels).

The Public Services Broker model is based on a hub architecture. Hubs at central, sectoral or local levels are used to exchange data to support common services at the appropriate level and sectoral data stores can be supported by central authentication and security services. This means data captured once can be reused by other agencies and on other occasions.

**Privacy issues in brokered identity**

In terms of privacy protection on a legal level, brokered identity must work within existing privacy law. In the Reach initiative, the program is being created within the framework of the Irish Data Protection Act \(^{13}\) and the Freedom of Information Act. \(^{14}\) The provisions of the Social Welfare Acts \(^{15}\) also contain safeguards for protection of the individual’s right to privacy (Department of Social, Community and Family Affairs 1999). Pivotal to the initiative is that users will have control over their personal information – they are given discretion over disclosure of their personal information to government bodies.

Furthermore, the Public Services Broker is independent of public service agencies, acting as both an ‘agent for customers and a shop-front for the Public Service’. \(^{16}\)

In terms of the practical mechanisms used to protect privacy, the Personal Public Services Number serves as the customer’s unique key which will help the development of personalised services and minimise the risks of error and inaccuracies in personal records. The customer will be able to deposit personal data with the Public Services Broker, and later choose to release it to a public service agency when applying for a service. \(^{17}\) This does not mean, however that a personal profile is going to be built on every person
in the country. Only the minimum data required for a particular transaction would be viewable by the staff member assisting the customer. The Broker would give the individual customer as much control as possible over the release of personal data from their personal data stores. All accesses to personal data will be recorded and staff will be unable to view personal profiles unless the customer grants permission by keying in a PIN or password (Irish Times 2001).18

A key issue for Reach (and brokered identity in general) is ensuring the community has a sufficient level of trust in the identity broker. This trust can be difficult to achieve, especially in communities where the government and private sector have a history of privacy intrusion and privacy abuse. In Ireland, the Reach initiative has attempted to win community trust through adoption of the following measures:

- **Legislation** already exists on collecting and storing personal information. In addition, creation and use of Personal Public Services Numbers and Public Service Cards is vested, by law, in the Minister for Social Community and Family Affairs.
- **Transparency** – To ensure people understand how personal data will be kept secure, the rules and procedures for collecting and releasing personal information will be published.
- **Oversight** – compliance with published procedures and legislation is further subject to scrutiny by a number of statutory position holders, namely the Comptroller and Auditor General, the Ombudsman and Information Commissioner and the Data Protection Commissioner.
- **Choice** – The Public Services Card (a smart card containing the Personal Public Services Number and other necessary personal identifiers) will not be a national identity card. It is designed to meet the needs of people to identify themselves when using public services. The new card does not have to have a photograph, date of birth or any other personal data. It could, for example, be like an ATM card, which when used with a PIN sufficiently identifies the person to draw down cash from ATM machines or carry out banking instructions. The key principle to be adopted is that customers choose the additional features to be added to their basic card.19

The Reach model aims to give consumers customised options for limiting the use of their data.

The Irish government, through Reach, has worked hard to design a privacy-friendly brokered identity system. Reach’s underlying philosophy of giving the consumer control over their personal information has enabled them to develop an effective one-stop-shop model of e-government that is founded on consumer, rather than government, control of information.

**The future for brokered identity**

Once fully implemented the Reach initiative could, subject to appropriate privacy protection, alter the way most people interact with and use government services. The one-stop-shop model will provide administrative efficiencies for both the public and the public service providers.

These benefits may include:

- connected services that will enable customers to access more than one service through a single access point
- personalised services that are founded on the individual needs of the customer and his or her preferences
- choice and convenience so customers will be able to choose the time and place which best suits them
- reduction in repeat form filling and provision of basic personal data
- simplification of access to services and information by allowing self-service over the Internet.
The Irish Government hopes the focus on privacy protection in implementing this initiative ensures these benefits will be achieved with negligible privacy intrusion. Other jurisdictions will be monitoring the Reach and the Public Services Broker implementations to assess their effectiveness and possible use in their own development of e-government services.

**Identity management and privacy**

Identity management strategies must include consideration of options that address privacy risks. The current trend is to build privacy protection into the technical design of distributed identity, and to develop solutions which differentiate between anonymous authentication and identification based on the requirements of individual transactions.

However, these design issues can be complemented by effective ongoing privacy management, including use of privacy management tools such as a privacy impact assessment, a privacy management strategy and/or ongoing privacy oversight.

**Privacy impact assessment**

A privacy impact assessment identifies privacy issues in specific sectors or applications. A privacy impact assessment process is particularly useful in implementations of new technology or new processes. By using the privacy impact assessment tool at the design stage of an implementation, organisations can avoid privacy errors and the costs of rectification later.

**Privacy management strategy**

A privacy management strategy is used to develop and implement a risk management strategy and practical action plan. Each privacy issue is allocated a response and action is delegated to individuals or organisations. A privacy management strategy would include a compliance timetable.

An important part of developing a privacy management strategy is the conduct of public and stakeholder consultations. These consultations are often as important as ensuring technical compliance. Effective consultation can help identify and manage key privacy risks.

**Ongoing privacy oversight**

Ongoing privacy oversight can be delivered by establishing a privacy oversight committee. This tool is used to develop a governance structure to oversee privacy issues arising throughout the life of the implementation. Some privacy issues may not be ascertained at the design stage so reviews and audits under the direction of an oversight committee are often necessary.

The broad functions of a privacy oversight committee can include making recommendations on new training initiatives, changes to documentation, changes to policies and procedures and changes to systems and design. A typical privacy management committee will have:

- an independent chair and a balanced membership
- the ability to make recommendations to the Board
- appropriate resources
- access to complaints statistics, details, audit reports and other relevant data.
References


Notes

1 Definition adapted from Pato & Rouault 2003.
2 <http://www.projectliberty.org>.
4 For further discussion of Liberty and privacy see Kaye 2002; Loftesness 2002; Migliore 2001.
9 <http://www.reach.ie>.
10 For more information about Reach’s goals, objectives and actions see Department of Social and Family Affairs 2002, p. 68; information about Ireland’s e-government agenda is on pp. 40–2.
18 See also <http://www.reach.ie/faqs.htm>, which notes the privacy protective features of the Public Services Broker scheme.
21 For example, Telstra had a Privacy Audit Panel for five years (1995–2000). The Panel was initially a legislative requirement and involved reporting to the Minister and the regulator. However, Telstra decided to keep the Panel in operation following de-regulation because they found it was a very useful tool in identifying privacy concerns.