THE UNIVERSITY OF NEW SOUTH WALES

galexia CONSULTING

Distributed Identity and Privacy - Case studies (September 2003)

Chris Connolly, Perter van Dijk, Prashanti Ravindra, Francis Vierboom

Distributed identity schemes are identification and authentication systems which operate as alternatives to national ID schemes, and might include federated identity or identity broking.

Distributed identity is being considered as a privacy positive alternative to national identification schemes (such as the failed Australia Card). The paper argues that while distributed identity may be a reasonable alternative to national identification 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.

These two case studies accompany a paper presented at the Baker & McKenzie Cyberspace Law and Policy Centre's "Surveillance and Privacy 2003" conference (Sydney, September 8-9) by Chris Connolly[1] That paper, "The privacy risks and rewards of distributed identity", discussed distributed identity management systems and proposed a set of privacy tools which can be used to assess and manage privacy risks in such systems.

Galexia Consulting continues to conduct research on distributed identity systems. These case studies and the accompanying power point presentation provide a brief introduction to the field.

This paper is available in the following formats from http://consult.galexia.com:

- The privacy risks and rewards of distributed identity – Presentation[2]
- Distributed identity - Case studies – HTML[3]
- Distributed identity - Case studies – PDF[4]

[1] Chris Connolly is a Director of Galexia Consulting, a specialist consulting firm which focuses on electronic commerce, privacy, authentication and identity management. Chris is also a Visiting Fellow in the Law Faculty at the University of New South Wales, where he teaches Electronic Commerce Law and Practice (amongst other courses) in the Masters Program and a Director of the Financial Services Consumer Policy Centre, a research centre affiliated with the UNSW

[2] PowerPoint version of conference slides:
<http://consult.galexia.com/public/research/assets/gc_distributed_identity_presentation_200309.ppt>
PDF Version of conference slides:
<http://consult.galexia.com/public/research/assets/gc_distributed_identity_presentation_200309.pdf>

[3] HTML version of paper: <http://consult.galexia.com/public/research/articles/research_articles-pa02.html>

[4] PDF version of paper <http://consult.galexia.com/public/research/assets/gc_distributed_identity_paper_200309.pdf>

Email: consult@galexia.com **Web:** consult.galexia.com **Ph:** +612 9555 5666 **Fax:** +612 9555 5688
Post: Level 1, 3 Montague St, Balmain (Sydney) NSW 2041, Australia

Contents

1. Case study – Reach

1.1. Overview

Reach is an agency established by the Irish Government in 1999 to develop a strategy for the integration of public services and to develop and implement a framework for e-government[5]. In May 2000 Reach was commissioned by the Government to procure the Public Services Broker (PSB). Since then, Reach has been focussed on defining and implementing the architectures and principles underlying the operation of the PSB[6]. 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.[7]"

As part of its work with the PSB project Reach is developing standards and legislation that will deal with issues of interoperability, Internet security and privacy. Reach's roles and objectives fall into three key areas:

- standards and operational policies[8];
- co-ordination and leadership[9]; and
- implementation and delivery of infrastructure and systems[10].

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, Reach is developing the Public Services Broker. The model seeks to balance the need for the maximum availability of data to public service agencies while ensuring the highest level of privacy and respect for data protection principles.

---

[5] <http://www.reach.ie>

[6] Department of Social and Family Affairs, *Statement of Strategy 2003-2005*, 2002, <http://portal.welfare.ie/publications/allpubs/strats/ss0305.pdf>

[7] For more information about Reach's goals, objectives and actions see p 68 of the Strategy document. Information about Ireland's eGovernment Agenda are on pp 40-2.

[8] See <http://www.reach.ie/about/what_is/standards.htm> for more information.

[9] See <http://www.reach.ie/about/what_is/coordination.htm> for more information.

[10] See <http://www.reach.ie/about/what_is/implementation.htm> for more information.

Another Reach service is the Inter-Agency Messaging Service (IAMS) which is currently being developed to support the electronic exchange of customer data among agencies in the public service[11]. The project recently received an Honourable Mention at the European Union e-Government Conference earlier this year[12].

Reach is implemented as an element of the Irish Government's broader eGovernemt strategy which aims to ensure quality of service to people dealing with government agencies and improvements in administrative efficiencies[13]. Reach is also responsible for ensuring that the development of electronic Government in Ireland is done in the context of European Union initiatives. This involves complying with the eEurope Action Plan[14] which sets the eGovernment strategy in the wider European context and places certain e-government development obligations on Ireland.

1.2. Public Service Broker

The PSB 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[15]. The PSB aims to improve delivery of services to the public through traditional means (in person and on the phone) and the new self-service electronic channel[16].

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); and
- 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 will be based on a hub architecture. Hubs at central, sectoral or local levels can be 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 that data captured once can be reused by other agencies and on other occasions. The individual's right to privacy will be protected by enabling them to know, and exercise control over, how their personal information is used.

The Public Service Broker is not a single application, rather it can be viewed as:

- a portal;
- a user access management system;
- a set of PSB user services;
- a set of PSB management services; and

[11] <http://www.reach.ie/iams/>

[12] <http://www.reach.ie/iams/winners.htm>

[13] <http://www.reach.ie/about/why_now/egovernment.htm>

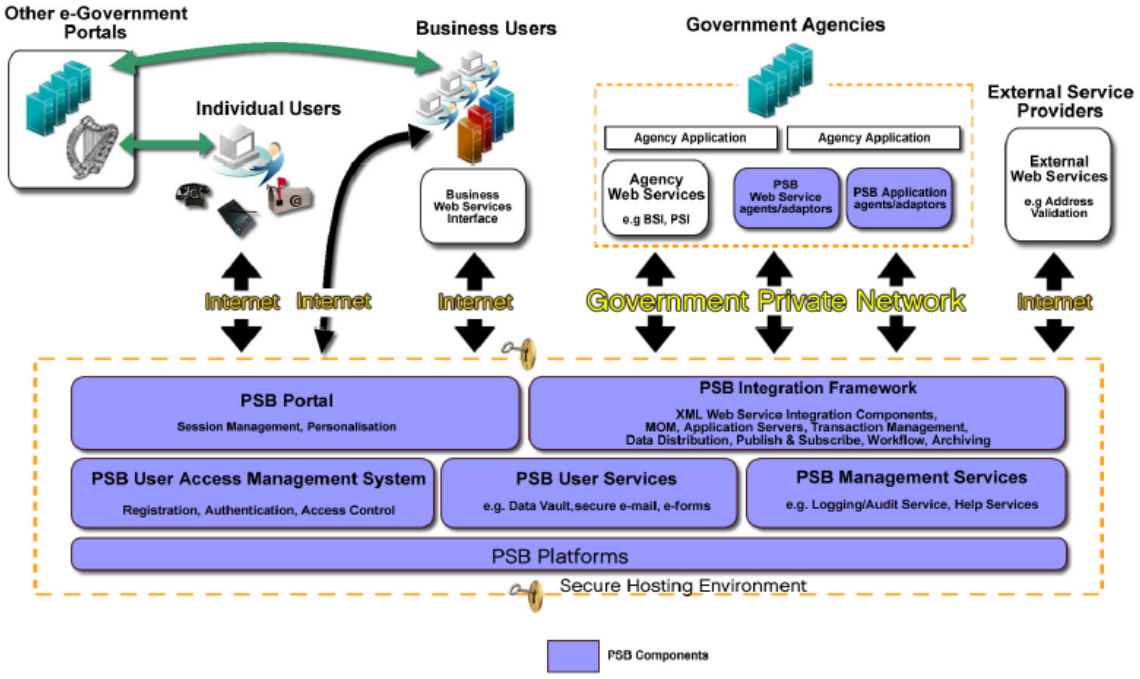
[14] <http://europa.eu.int/information_society/eeurope/action_plan/index_en.htm>

[15] **reach** services, *Public Services Broker Phase 1 Requirements Statement*, 11 July 2002, <http://www.reach.ie/psb1/Requirements_Statement.pdf>

[16] Irish Internet Association, 'Ireland's eGovernment - Reach Services', *New Perspectives*, November 2002, <http://newperspectives.iia.ie/e_article000109297.cfm>

— an integration framework - a set of components and tools that will be used to integrate the above services and to PSB-enable Government services.

The complexity of the PSB and its role in the provision of e-government services is represented in the diagram below:



High Level Schematic view of PSB architecture[17]

1.3. Current status

The development and implementation of the PSB and other components of the eGovernment strategy are behind schedule[18]. At present Reach is continuing to develop and refine requirements and policy documents for its various projects, including the Inter-Agency Messaging Service, and in particular the PSB.

In June 2003 Reach announced that it had selected four suppliers to continue developing the PSB in the procurement process[19]. A final supplier is expected to be announced in November 2003 and will implement the Broker in light of Reach's technical specifications[20].

The **reach**services website[21] was launched in April 2002 and is intended to be the single gateway to government services online. It is a significant component of Ireland's centralised model of e-government.

---

[17] p 4, **reach** services, *Public Services Broker Phase 1 Requirements Statement*, 11 July 2002, <http://www.reach.ie/psb1/Requirements_Statement.pdf>

[18] See Clark, Matthew, 'Hannifin acknowledges e-government delays', *ElectricNews.net*, 17 February 2003, <http://www.enn.ie/news.html?code=9350157>, and Interchange of Data between Administrators, *Irish e-government strategy experiencing delays to implementation*, 18 February 2003, <http://europa.eu.int/ISPO/ida/jsps/index.jsp?fuseAction=showDocument&documentID=875&parent=chapter&preChapterID=0-140-194-329-338> for more information.

[19] Reach, 'Progress Update on the Public Services Broker', *Press Release*, 20 June 2003, <http://www.reach.ie/new.htm>

[20] Ibid.

1.4. Privacy issues

In terms of privacy protection on a legal level Reach initiatives are being created within the framework of the *Data Protection Act* and the *Freedom of Information Act*. The provisions of the *Social Welfare Act* also contain safeguards for the protection of the individual's right to privacy[22]. Pivotal to the initiative is that users will have complete control over their personal information. They will be given absolute discretion over disclosure of their personal information to the government bodies.

In terms of the practical mechanisms used to protect privacy the Personal Public Service Number (PPSN) 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[23]. 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[24].

The FAQ section on the Reach website addresses some common privacy concerns held by the public about the Reach initiative, noting that:

> The Public Services Card [a smart card containing the PPSN and other necessary personal identifiers] will not be a national identity card. It's designed to meet the needs of people to identify themselves when using public services. The new card doesn't 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 we are adopting is that customers choose the additional features that can be added to their basic card.[25]

The Reach model aims to allow the great bulk of privacy-neutral citizenry to transact fairly freely with agencies while giving others customised options for limiting the use of their data.

1.5. Commentary

The Irish government through Reach have worked hard in trying to create a privacy friendly identity brokering system, and to a large extent have succeeded in this endeavour. Reach's underlying philosophy of giving the user total control over their personal information enables them to come up with an effective 'one stop shop' model of e-government that is founded on user rather than government control of information.

---

[21] <http://www.reachservices.ie/static/index.htm>

[22] Department of Social, Community and Family Affairs, Establishment of National Framework for Integration of Public Services – 'Reach', 31 August 1999, <http://www.cidb.ie/Live.nsf/0/4b45f6c7db25df87802567e6004dbf21?OpenDocument>

[23] <http://www.reach.ie/about/achieve/privacy.htm>

[24] Irish Times, *Data Protection Essential for e-Government plan*, 9 September 2001, <http://www.cidb.ie/live.nsf/0/41b883a289b58c4880256b17005399e0?OpenDocument&ExpandSection=7>. See also <http://www.reach.ie/faqs.htm> which notes the privacy protective features of the PSB scheme.

[25] <http://www.reach.ie/faqs.htm>

However, there are a couple of hurdles that Reach are yet to overcome. Firstly, the implementation of the PSB is severely behind schedule; and secondly it appears that the public are yet to overcome privacy fears about the Internet.

The majority of Irish people (56%) feel that 'if you use the Internet your privacy is threatened'[26]. This could have disastrous ramifications for the PSB and other e-government initiatives. Despite Reach's priority of user data control, these efforts could be rendered useless if the public cannot be inspired to use the services once they have been developed[27].

1.6. Future potential

Once fully implement the Reach initiative, and in particular the PSB could alter the way most people interact with and use government services. The centralised, one-stop shop model will provide administrative efficiencies for both the public and public service providers. It is also argued that the initiative also has the potential to better accommodate less able or computer literate people such as the elderly, as government agencies will be better resourced to handle these people's needs face-to-face or over the phone.[28]

In general the Reach initiative once fully implemented is expected to provide a number of benefits to government services including:

- Connected services 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;
- Provide choice and convenience so that customers will be able to choose the time and place which best suit them;
- Reduce repeated form filling and provision of basic personal data;
- Simplify the access to services and information by allowing self-service over the Internet.

The Irish Government hopes that the focus on privacy protection in implementing this initiative ensures that the above points will be achieved with negligible privacy invasion.

1.7. Additional References

1.7.1. Terms of reference

Reach's terms of reference is to:

- Develop the framework for delivering integrated public services to individual customers and businesses in Ireland.

[26] Data Protection Commissioner, 'Privacy Fears on the Increase, warns Data Protection Commissioner' *News Release*, 13 January 2003, <http://www.dataprivacy.ie/7nr130103.htm>

[27] See McDonald, 'Privacy concerns balloon in Ireland', *ElectricNews.net*, 16 January 2003, <http://www.enn.ie/news.html?code=8894120>

[28] Irish Internet Association, 'Oliver Ryan, Director of Reach Services', *News Perspective*, 13 November 2002, <http://newperspectives.iia.ie/e_article000107741.cfm>

— Develop and implement the framework for electronic delivery of public services - the "eGovernment" and Information Society agendas.

— Co-ordinate the eGovernment programme across the Public Service.[29]

Reach's mandate 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 will be done in consultation with Public Service delivery agencies and customers.

— Develop the existing Public Services Card as the customer's secure key to accessing public services.

— Promote the use of the Personal Public Service Number (PPS No.) - formerly the RSI Number - by the public and by authorised Public Service agencies.[30]

1.7.2. Reach's Legal Framework

Reach was established by Government decision in 1999 and its mandate extended, again by Government decision in 2000, to develop the Public Services Broker.

Reach grew out of the Integrated Social Services Strategy adopted by the Government in 1996 that recommended the integration of public services, increased sharing of data and the extension of the use of the RSI Number across the public service in the interest of improving customer service.

The legal framework for the sharing and use of essential personal data is set out in a number of Acts, viz. Data Protection Act, 1988, Social Welfare Acts, 1998, 1999 and 2000 and Social Welfare (Miscellaneous Provisions) Act 2002 (see Resources for text); and the Health Act, 1997.

The Minister for Social, Community and Family Affairs, whose Department is responsible for the issue of Personal Public Service Numbers and the Public Services card, reports to Government on the progress of the Reach initiative.

1.7.3. Reach's Inter-Agency Messaging Service

Reach developed the Inter-Agency Messaging Service (IAMS) to support the electronic exchange of customer data among agencies in the public service. The IAMS will initially allow the exchange of birth registration data between the GRO and the Department of Social and Family Affairs' Client Identity Services Section (CIS), and between the GRO and the Central Statistics Office (CSO). This service will eventually be extended to support the capture and dissemination of death and marriages notification data among a wider range of agencies.

See <http://www.reach.ie/iams/> for more information.

1.7.4. reachservices

reachservices <http://www.reachservices.ie> is a public sector e-Government initiative delivered by the Reach Agency.

[29] <http://www.reach.ie/archive.htm>

[30] Ibid.

> "The Irish Government established the Reach Agency in 2000 to develop a strategy for the integration of public services and to develop and implement a framework for electronic government. **reachservices** was developed with this goal in mind and is designed to offer you a single gateway to government services online.
>
> reachservices provides you with quick, secure access to public sector information and interactive services. We also feature a wide range of application forms for public services delivered by various public sector bodies - Government Departments, State Agencies, Local Authorities and the Health Sector."

See also <http://www.reachservices.ie/static/faq.htm>.

1.7.5. Ireland's plans to record life events

Refer to an article on plans to record life events including registration of marriages at <http://www.examiner.ie/pport/web/ireland/Full_Story/did-sgILwte06mVG6sgdL11Zs5FWAE.asp>.

2. Case study - Liberty

2.1. Overview

Liberty Alliance[31] 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.

It employs the concept of 'federated identity', where (the concept supposes) 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, of course, applicable privacy and data protection laws.

Liberty incorporates a number of thoughtful and effective measures with regard to technical aspects of privacy, such as anonymous cross-site authentication. But it rightly asserts that it cannot enforce many policy aspects of privacy on its users.

Given that the development of such a standard seems to be inevitable, this paper considers the effect of the Liberty Alliance specification on privacy and how associated privacy risks can be addressed.

2.2. History

A way of uniformly identifying users across the Internet has haunted the dreams of marketing directors and the nightmares of privacy advocates. However, for a long time the financial costs of such a system were prohibitive, given the marginal benefits.

Unsurprisingly, Microsoft, ever the long-term investor and innovator, was the first company to make a foray into such an identity system. Code-named 'Hailstorm' – already a fatal mistake – it proposed a vast Microsoft-controlled database where the user registered all their details once and could then browse the web seamlessly.

It was the momentum of both consumer and corporate opposition to the Hailstorm concept that gave birth to the 'Liberty Alliance' in September 2001, a consortium of major companies spearheaded by Microsoft competitor Sun Microsystems. The group explicitly aimed to provide an alternative and more privacy-friendly system by creating a specification for managing a 'federated network identity'.

Phase 1 of the Liberty Specification was released in July 2002, revised to version 1.1 in January 2003, and revised to v1.2 with the release of Phase 2. It only dealt with the basic cross-site authentication feature of the system, allowing users to navigate among different sites without signing in to each with a password, and did not describe any system for exchanging personal information.

The Phase 2 draft was released in April 2003 and a revision in August 2003. This module outlines more significant Liberty features – the permission-based sharing of information.

[31] <http://www.projectliberty.org>

2.3. Technical outline

Refer to *Liberty Alliance Phase 2 Draft Specifications* at <http://www.projectliberty.org/specs/>

2.3.1. Enhancements to Phase 1, the Liberty Identity Federation Framework (ID-FF)

The Liberty Identity Federation Framework version 1.2 provides new functionality to the opt-in account linking and single sign-on capabilities released in July 2002. ID-FF version 1.2 now includes protocols for the following features:

- **Affiliation:** This enables a user to choose to federate with a group of affiliated sites, a critical need for portals and business-to-employee applications.
- **Anonymity:** This enables a service to request certain user attributes without needing to know the user's identity[32].

2.3.2. Introduction of the Liberty Identity Web Services Framework (ID-WSF)

The Liberty Identity Web Services Framework outlines the technical components necessary to build interoperable identity-based web services. Specific features include:

- **Permissions-Based Attribute Sharing:** This allows an organisation to offer users individualised services based on attributes and preferences that the user has chosen to share.
- **Identity Discovery Service:** This allows a service provider to dynamically discover the location of a user's identity services, and for the identity provider to respond based on the user's permissions. This feature is critical for being able to offer a large number of users real-time identity-based services.
- **Interaction Service:** This allows an identity service to obtain permission from a user (or someone who owns a resource on behalf of that user) to allow them to share data with the requesting service.
- **Security Profiles:** This describes the profiles and requirements necessary to protect security and ensure the integrity and confidentiality of messages.
- **Extended Client Support:** This enables hosting of Liberty-enabled identity-based services on devices without requiring HTTP servers. This is useful since most consumers do not run HTTP-servers on their PCs, and many networks do not support running HTTP-servers on consumer devices. This also reduces implementation costs in resource-constrained devices such as mobile phones.

2.3.3. Introduction of the Liberty Identity Service Interface Specifications (ID-SIS)

In Phase 2 and future phases of its specifications, the Liberty Alliance will be developing a collection of specifications, built on the Liberty Identity Web Services Framework, that offer companies a standard way to build interoperable identity-based services. The first of these is:

- **ID-Personal Profile:** This service defines a template for basic profile information, typically used in registration. It includes a standard set of attribute fields (name, legal identity, legal domicile, work address, email address) so organisations have a common language to speak to each other and offer interoperable services.

[32] <http://xml.coverpages.org/ni2003-04-15-b.html>

2.4. The challenges for Liberty

The challenge for online authentication systems is that they have not yet reached the stage where they offer practical benefits and applications to consumers. A 2002 Gartner report[33] found that people are generally distrustful of, and uninterested in, broad online authentication systems. Liberty members seem to hope that consumers will be attracted to federated identity because of problems with existing authentication systems:

> Fast-forward to the grown up and modern world, pieces of their identity are now scattered across an endless list of entities; banks, credit card companies, brokerage firms, insurance companies, national IDs, pension funds, medical providers, and the places where they work. The Internet has become one of the prime vehicles for business, community and personal interactions, and it is fragmenting this identity even further. Pieces of their identity are doled out across the many computer systems and networks used by employers, Internet Service Providers, bulletin boards, instant messaging applications, and online commerce and content providers. This all occurs with little coordination, interaction, or control on their part.
>
> The result is a fairly high level of frustration for everyone involved. People have to repeatedly enter the same information within the workplace and in personal business dealings. The IT manager must provision dynamically changing accounts to reflect up-to-date roles and identities within the organization. The sales executive needs to reach the audience with the right identities to sell a product.[34]

Despite the picture painted by this passage from a Liberty document, the broad usage of Liberty in retail e-commerce seems a long way off. Given some consumer resistance, the expense of deployment and the limited benefits that such systems can bring, it's hard to imagine Liberty becoming a pervasive standard on the Internet in the medium term.

The more viable – and less privacy intrusive – applications are for more discrete networks of users and providers. 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 not much personal information is needed, and the usability benefits are significant:
- **Student and employee intranets** – large companies and universities often have a number of separate internal IT 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; and
- **e-government** – although the risks of identity fraud are significant, governments are generally regarded as more trustworthy keepers of personal information than corporations, and the efficiency and cost savings from integrating various government departments are 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 considering the future benefits of Liberty, and backing the Liberty Alliance:

---

[33] <http://zdnet.com.com/2100-1105-892838.html>

[34] <http://www.projectliberty.org/resources/whitepapers/LAP Identity Architecture Whitepaper Final. PDF>

> 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.[35]

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

- **Identity theft** – by allowing a single authentication at a superannuation website to give a user access to insurance, banking and trading services, single sign-on systems increase both the vulnerability and incentive to identity thieves. The situation is exponentially worse as the system spreads across broader e-commerce sectors.
- **Targeted marketing** – as seen in the passage above, Liberty supporters openly anticipate trading in personal information with each other to profile their consumers.
- **Co-branding** – by setting up circles of trust within specific groups of related but non-competing companies – for example, the ubiquitous example traveler who books a flight and then clicks on the link to the car rental company – Liberty has the potential to encourages the reduction of free market competition.

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

2.5. The future for Liberty

Accepting that some form of online authentication system is all but inevitable, Liberty Alliance actually becomes an attractive option for privacy advocates. This is especially true given the only other major service in the area – the Microsoft Passport.

Passport, which Windows XP, Hotmail and MSN Messenger users have to sign up for, already has over 200 million subscribers, claims Microsoft[36].

However a Gartner study[37] from April 2002, which acknowledged the same Microsoft 200 million figure, estimated that there were only 25 million active Passport users, and only 60% of those were aware that they even had something called a Passport.

Passport is billed as a consumer service for e-commerce websites. If they so choose, Passport holders store their names, addresses and credit card numbers in a 'wallet' and use that as a one-step method of payment at Passport-enabled e-commerce sites.

As mentioned above, it was the outcry at Microsoft's ambitions over web identities that led to the Liberty Alliance, and it set out to create a privacy-friendly way of challenging Passport. While the systems are in competition to a degree, they are fundamentally different in a number of significant respects.

---

[35] <http://www.projectliberty.org/press/releases/2003-07-09.html>

[36] <http://www.microsoft.com/net/services/passport/business.asp>

[37] <http://news.com.com/2100-1001-892808.html>

Liberty Alliance is, most importantly, decentralised. While Microsoft is in control of the details of every Passport user, and every corporation that adopts the Passport service must rely on Microsoft, the Liberty Alliance federated identity model is based on allowing different companies to consistently interact with each other to discover a user's identity.

Conversely, and as envisioned above, this means that privacy protection is partially in the hands of individual companies within the Liberty system – some of whom may have a strong interest in abusing privacy and fly under the radar of any supervisory authority until it is too late. Note that Microsoft's system is under the close watch of the US FTC following the settlement of a suit regarding misleading statements in its privacy and security policies.

Liberty Alliance must now take some responsibility for providing comprehensive guidelines and promoting good privacy among its members[38]. The success of Liberty's concept of 'federated network identity' rests on its ability to ensure that information sharing does not run rampant over the interests of consumers.

[38] For further discussion of Liberty and privacy see:
<http://www.rds.com/essays/20020904-liberty.html>
<http://www.glenbrook.com/opinions/liberty-critique.html>
<http://www.esj.com/news/article.asp?editorialsId=75>