Government Support for an User Centric Electronic Identity System

The inquiry asks:

Develop a national strategy for promoting trusted digital identities, in consultation with financial institutions and other stakeholders.

The Inquiry seeks further information on the following areas:

- *In developing a national strategy, what should be the respective roles, responsibilities and expectations of Australian public and private sector organisations in creating, accepting and maintaining the digital identities used by Australians?*
- *Is there a need for Government to enhance identity authentication by facilitating interoperability standards in areas such as biometrics, enabling better access to Government information or improvements to the Documentation Verification Service?*

This submission recommends the government provide the leadership to allow individuals to have their own set of digital identities that they control and that they can use. One way of achieving this is to base digital identities around online behaviour collected by the individual themselves. This approach is behind the MIT Open Mustard Seed, part of the IDCubed.org project.

This approach turns identification around. The traditional approach to identification is based around organisation supplied credentials. An individual provides an organisation with identity evidence, which the organisation checks and then provides the individual with a credential. An alternative approach is based around an individual checking their own credentials. The individual proves, in an independently verifiable way, that their credentials are valid. The individual uses the same techniques and tools used by organisations. The individual then provides their credentials to the organisation.

People engage trusted third parties to supply the tools to record their verifiable behaviour. This is achieved by giving the individual electronic access to their information stored in their interactions with organisations through the trusted third party, where the person and an organisation trust the third party. Australian Privacy Principle 12 provides the legal framework for this to occur. APP 12 states

> ***APP 12 - Dealing with requests for access***
>
> *12.4 The APP entity must:*
>
> > *2. give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.*
>
> *and*
>
> *12.6 Without limiting subclause 12.5, access may be given through the use of a mutually agreed intermediary.*

Through the use of Open Standards there can be many trusted third parties used by persons and organisations.

This change in approach leads to systems that are private by design. The following privacy principles are built into the identity operation.

Australian Privacy Principle 5 (APP 5) - Notification of the collection of personal information

The individual input their own personal information and hence are automatically notified.

APP 6 — Use or disclosure of personal information

The individual approves and controls all disclosure of personal information

APP 7 — Direct marketing

The individual must approve all direct marketing coming from the use of their information.

APP 9 — Adoption, use or disclosure of government related identifiers

Government identifiers are only used by the individual for their own identification and that use of government identifiers is permitted.

APP 10 — Quality of personal information

Because the individual is responsible for their own information and because they have tools to assist in the gathering and checking of information the quality is high.

APP 12 — Access to personal information

The individual has access to their personal information by design.

APP12 also says that a person can ask for their information in any way they wish and can engage a third party agreed to by an organisation, to act as their agents.

APP 13 — Correction of personal information

The individual is able to correct their personal information.

Creation of a User Centric Identity Systems

The first step in creating a User Centric Identity System has been in operation in Australia since 2008 and is operated by the Company Edentiti under the brand greenID. Edentiti uses the Document Verification Service (DVS) to give people access to their identity credentials held by government agencies through organisations. That is, the DVS only allows organisations who are required under Federal Legislation to identify people to use the system. Such legislation is the AML/CTF legislation and the Telecommunications ACT. Requests to the DVS to allow an individual to access their own records through the DVS using an agreed trusted third party have been denied. A simple enforcement of the Federal Australian Privacy Principle 12 would immediately increase the demand for the DVS service and make the DVS available to any organisation who has a need for identification.

The experience with the DVS illustrates the issues associated with a person getting access to their own government data (and personal data held by organisations). The problem is that the government deals with individuals through other organisations and not directly with individuals. Changing the paradigm where the government deals directly with individuals via a third party agent selected by the individual designs privacy into the system. When the government uses organisations it appoints to deal individuals privacy has to be tacked on to the system.

By allowing the individual to have a choice in how their identity information is accessed will immediately simplify almost all government to citizen engagement. This happens because if the individual can access their own information held by government then they can supply it to other parts of government and to other organisations.

The approach does not invalidate existing systems. They can continue to operate almost exactly as they currently operate. The big change is that individuals can immediately start to reuse their previous electronic activity not only for identification but for other transactions. It means that a person need only ever record data or biometrics once and then continue to reuse it. The practical effects are to eliminate the need for

- every organisation to have its own username/password system
- complex negotiations and agreements between organisation on the passing of information between organisations,
- a person to continually re-enter information about themselves

If the government provides a lead by allowing individuals, through trusted third parties, to access their own information other organisations within society will follow their lead and will give individuals access and some control over information about themselves. This will be privacy friendly.

Very large savings will be made in ehealth, tax collection, distribution of entitlements to citizens and organisations.

Recommendation

The government develop a national identity strategy around the idea of supporting and encouraging individuals to access their own personal data held by government. As the first step the government should require all government agencies to follow APP12 and allow individuals access to information about themselves held by government agencies through mutually agreed third parties.

Kevin Cox August 2014