Submission by the Australian Communications Consumer Action Network to the Department of Prime Minister and Cabinet's consultation on a National Trusted Identities Framework

October 2012

About ACCAN

The Australian Communications Consumer Action Network (ACCAN) is the peak body that represents all consumers on communications issues including telecommunications, broadband and emerging new services. ACCAN provides a strong unified voice to industry and government as consumers work towards availability, accessibility and affordability of communications services for all Australians.

Consumers need ACCAN to promote better consumer protection outcomes ensuring speedy responses to complaints and issues. ACCAN aims to empower consumers so that they are well informed and can make good choices about products and services. As a peak body, ACCAN will activate its broad and diverse membership base to campaign to get a better deal for all communications consumers.

Contact

Steven Robertson

Suite 402, Level 4
55 Mountain Street
Ultimo NSW, 2007
Email: info@accan.org.au
Phone: (02) 9288 4000
Fax: (02) 9288 4019
TTY: 9281 5322

Contents

Executive summary

At this point in the development process, ACCAN cannot support the NTIF. There are several reasons for this, primarily related to the consultation process and the need for greater information, transparency and consumer focus. The key points raised in ACCAN's submission are:

- The benefits of the NTIF to consumers have been insufficiently addressed—no adequate "business case" for consumers has been put forward;

- The NTIF introduces a number of risks to consumers, and consumer concerns about these risks should be acknowledged and addressed;

- The consultations thus far have had a strong business presence, and more emphasis on the benefits to consumers is needed to alleviate concerns that the NTIF is simply a tool for business and governments to better identify individuals;

- A great deal of discussion during the October consultations focused on the extension of the Document Verification Service (DVS) to use by private sector organisations, and this proposal would undercut many of the claimed consumer benefits of the NTIF;

- Much more detail about the NTIF is needed for consumers and civil society representatives to be able to engage with the development process, and this detail should be made public and provided in a timely and transparent manner if there is to be any confidence in the process from civil society and consumers; and

- Certain consumer protection measures that have been referred to during earlier rounds of consultation should be reinforced to ensure consumer and civil society trust and confidence.

The NTIF consultation process

It should be noted at the outset that the consultation process for the NTIF appears to be at an early stage. In particular, there appears to be no technical or governance detail about the NTIF, and no detailed analysis of the potential risks and benefits of the NTIF. As a result, this submission is quite general in nature.

We are concerned that civil society groups appear to have been under-represented at this stage of the consultation. While we understand that this is in part a result of the NTIF consultations being at an early stage, it is essential for building consumer trust and confidence in the NTIF that consumer interests are well-represented as the NTIF development continues, that consultations are open and transparent, and that all consultation documents are made publicly accessible where possible.[1]

As a consequence of the over-representation of business interests during the consultation, a great deal of the discussion in the October plenary sessions focused on the extension of the Document Verification Service (DVS) to private sector organisations. While the DVS extension in itself is outside ACCAN's purview, we are concerned that the NTIF consultations have to some extent been reduced to questions of the DVS extension. The claimed benefits of the NTIF extend beyond private sector interests, yet the DVS extension would primarily benefit businesses. If the DVS extension is to serve as the next stage in the development of the NTIF it will likely undermine consumer confidence in later stages of the NTIF.

ACCAN is also concerned that the NTIF has not yet been adequately justified. In particular, although the value of the NTIF appears to have been presumed, there has been no clear case made from a consumer perspective that the NTIF is needed. We note that the lack of an adequate business case has been identified as one of the reasons for failure of government ICT projects.[2] A business case should identify the benefits to consumers as well as business. This business case should be made before the NTIF project proceeds, with the results of the analysis made public.

In addition to these concerns about the consultation process, there are a number of consumer issues present in the NTIF discussions to date, which are addressed below.

[1] We note, on this point, that the Cyber White Paper website is no longer available at <http://www.cyberwhitepaper.dpmc.gov.au/>, and that the consultation documents appear to be publicly available only through the Australian Privacy Foundation's website.

[2] Victorian Ombudsman, *Own motion investigation into ICT-enabled projects*, November 2011, pages 22—27, <http://www.ombudsman.vic.gov.au/resources/documents/Investigation_into_ICT_enabled_projects_Nov_2011.pdf>.

Consumer concerns

The NTIF consultation documents indicate some potential benefits to consumers. While ACCAN recognises (and supports) these benefits, we note that there are also a number of consumer concerns that must be addressed if there is to be consumer trust and confidence in the NTIF.

1. Pilot projects and the DVS

During the October 2012 consultation process, there appeared to be a consensus among private sector and government representatives that a pilot project was needed in order to trial and assess some of the possible models for the NTIF. ACCAN recognises that a pilot project would be a useful way to test the effectiveness of a trusted identities system in a limited way. Before any project is conducted, however, there should be a greater disclosure of information about the nature and purposes of the pilot.

During the October 2012 consultations, a great deal of discussion centred on the expansion of the Document Verification Service (DVS) to private sector organisations. The view from industry appeared to be that the DVS extension would be a suitable pilot project for the NTIF. ACCAN disagrees, and suggests that an alternative pilot project should be used. Any extension of the DVS is more appropriately dealt with alongside the NTIF pilot project, rather than as a replacement for it. The key reasons for this view are:

- The extension of the DVS will primarily benefit private sector organisations. This is not in keeping with the stated purposes of the NTIF, which included allowing consumers and citizens to verify identity and attribute information about organisations. Although there may be some incidental benefit to consumers in private sector organisations having access to more accurate data, the NTIF program should not be reduced to the implementation of the proposed DVS extension.

- The DVS extension proposal has been developed with little to no involvement from consumer and civil society groups. Indeed, the privacy impact assessment for the DVS extension proposal was not available to the public until a few days before the final stage in this round of consultations.

- As a first step towards the NTIF, any extension of the DVS—a service which benefits organisations but which is unavailable to individuals—would only serve to reinforce the perception that the primary beneficiaries of the NTIF are businesses and government agencies rather than individuals. This would adversely affect consumer trust and confidence in the NTIF.

Any consideration of possible pilot projects should include a transparent consultation process. This should include an identification of benefits and risks of the pilot project, and an explanation of how they address the stated NTIF goals (such as enhanced privacy, enhanced security, ease of use, etc). Such an approach would be useful not only in identifying a suitable pilot project but also in identifying in a concrete way some of the possible benefits of the NTIF.

2. Consumer trust

The central claimed benefit of the NTIF is an increase in online trust. The 2012 consultation document notes that:

> To do business or provide services effectively online, organisations (including governments) need to be sure that the person they are dealing with is trustworthy. At the same time, for people to fully participate in the online economy, they need to trust organisations and service providers. Both need to feel comfortable with and understand security and privacy arrangements.[3]

To ensure that this benefit is realised, it is important that consumers have confidence in the NTIF itself. To this end, several issues need to be addressed.

2.1 Explanation of consumer benefits

The NTIF potentially offers a simple method for users to verify the identity of organisations with which they conduct their online transactions, and this may lead to better consumer protection against online fraud, scams, phishing attacks, and so on. More needs to be done, however, to illustrate the potential trust benefits of the NTIF. It is not clear, for instance, what benefits (if any) the NTIF would offer over existing technologies for consumers wishing to verify the identity of a government agency or business.

The benefits to trust of the NTIF over existing trust tools need to be set out in greater detail. The 2012 consultation document describes several problems with existing trust tools:

> Organisations and government agencies build their own solutions for delivering trust, each with its own user name and password or other mechanisms for administering it. Each solution has its own checks to verify identity and many ask for more identity information than they need about a person. While these solutions meet the separate needs, they are not designed to be interoperable and cannot easily share resources.
>
> In turn, people must use each solution separately and often in very different ways. People need to manage an array of credentials, including usernames, passwords and cards. They have little or no control over what identity and other personal information they are asked to provide for accessing services. Once the information is given, they have little visibility over what it is being used for, who accesses it, or where to go when there is a problem. For many people this is annoying or unsettling but for some this is just too high a price to pay for online services.[4]

However, the document does not describe the ways in which the NTIF might mitigate these problems. While it is true that a federated identity system might offer some benefits to consumers (a single sign-on portal, for instance, can limit the need for multiple usernames and passwords) future phases in the development of the NTIF will need to identify the specific ways in which the NTIF will respond to the trust problems facing consumers.

[3] Information Integrity Solutions, *National trusted identities framework (NTIF) discussion paper*, 26 September 2012, page 3.

[4] Information Integrity Solutions, *National trusted identities framework (NTIF) discussion paper*, 26 September 2012, page 3.

2.2 Sources of identity and attribute data

The sources of attribute and identity data will impact on levels of consumer trust. Consumers are more likely to trust in identity information issued by government, for instance, than in identity information issued by private sector. While some situations will call for attribute and identity information to be issued by private sector (for example, in a consumer's dealing between a bank and a credit reporting agency) an over-reliance on private sector identity information will no doubt lead to a public perception that the NTIF is driven by business needs and that consumers are a product rather than an intended beneficiary.

2.3 Role of consumers and organisations

We also note that, from a consumer trust perspective, it is important that the NTIF recognise businesses and government agencies as users of the same standing as individuals. The focus of the NTIF should not be on verifying individuals (despite much of the discussion during the October 2012 rounds leaning in this direction). Individuals must be able to verify the identity of businesses and government agencies just as businesses and government agencies are able to verify the identity of individuals, and this function of the NTIF should remain clearly visible in future discussions.

The risks of failing to emphasise the consumer benefits in verifying organisations include a loss of consumer confidence in the NTIF. If the NTIF is perceived as primarily a means for government and business to better identify consumers it is likely to lose consumer support, and this support may be difficult to win back.

3. Nature of identities

The NTIF discussions to date do not appear to discuss the nature of online identity. ACCAN's view is that this is a significant issue that should be addressed in the initial stages of the NTIF development.

3.1 Online identity is multifaceted

The Framework must recognise that online identity is multi-faceted, and continue to allow individuals to maintain multiple identities.[5] Although there may be a legitimate need in some cases for two organisations to be sure they are dealing with the same individual, or for two individuals to be sure they are dealing with the same bank, there are many scenarios in which one individual or organisation has a legitimate reason to maintain multiple online identities:

- An individual dealing with one organisation in two distinct roles, e.g. as an individual and as a representative of a company;
- An individual dealing with multiple unrelated organisations, e.g. an online merchant and an online community group;
- An individual dealing with multiple organisations in different contexts, e.g. a government agency and a social networking site; and

[5] The seminal work on this point is Kim Cameron, *The laws of identity*, 8 January 2006, <http://www.identityblog.com/?p=352>; see also Stephen Wilson, *Let's embrace identity plurality*, 14 May 2012, <http://lockstep.com.au/blog/2012/05/14/identity-plurality>.

- An organisation dealing with different parties in different roles, e.g. the government and its shareholders.

We note that the name "National Trusted Identities Framework" suggests that identity will be multi-faceted in this way, however the nature of identity should be made explicit in future stages of consultation.

3.2 Disclosure of identity information

It is important to establish that disclosure of identity is not needed in many scenarios. It is often sufficient to acknowledge that a person is authorised for some action or that some condition is met. If, for example, it is sufficient for some purpose to verify that an individual is over 18, there should be no disclosure of the individual's date of birth, but rather a simple acknowledgement that the individual is over 18.

4. NTIF Principles

During the 2011 NTIF Consultation round, a number of guiding principles were discussed:

> [PM & C's draft policy proposal] proposes principles that could guide the development of a national trusted identities framework or market. These are that it should be:
>
> - voluntary, user-controlled and federated
> - strengthen participants' privacy
> - fit for purpose and easy to use
> - accessible and equitable
> - have national reach and support interoperability across industry, states and territories, the Commonwealth and internationally
> - support the development of a market driven by individuals and industry
> - balance risk appropriately across participants and
> - support innovation and competition, while remaining technologically neutral.[6]

The current consultation round included reference to an additional principle:

- allow individuals, businesses and governments to authenticate and mutually recognise each other's digital identities.

These principles, in ACCAN's view, are useful and appropriate. However, the principles appeared to have a reduced presence in the current consultation round—the principles were mentioned during IIS's presentation, but did not appear at all in the current consultation document.

[6] Information Integrity Solutions, *Private sector consultation on a market for a national trusted identities system*, 9 December 2011, page 3.

Given the limited detail currently available about the design and specifications of the NTIF, we feel it is particularly important to emphasise these principles throughout future consultation on and development of the NTIF. The principles indicate important consumer protection issues that might otherwise take a secondary position to business interests, increasing the trust that is essential to encouraging consumer involvement in the NTIF.

ACCAN also recommends that the principles be extended to explicitly recognise a right of contestability. In the event that an organisation presents incorrect data about an individual, the individual should have a simple and efficient mechanism available to challenge the data. The scope for incorrect data to cause problems for individuals is large, and might include, for instance, a "negative acknowledged" response caused by of a simple typo in an organisation's records.

5. Further issues

5.1 Accessibility

Many consumers face challenges in accessing ICT services.[7] The design of the NTIF should be such that the barriers to using its features are minimised, making the NTIF available to all users regardless of financial circumstances, geographic location, cultural or linguistic background, disability, or technical ability.[8]

5.2 Function creep

During the October consultations it was indicated that the NTIF is not intended to function as a national identifier (thus, perhaps, avoiding the concerns raised by the Australia Card or the Access Card). Nevertheless, many of the concerns raised by national identifiers are likely to be voiced by the community about the NTIF. Measures should be taken to reduce the possibility of identity information in the NTIF market being used in this manner.

5.3 The term "market"

The reference to an "identities market" is likely to generate some community concern. The term suggests that identity information will be traded as a commodity, a practice to which consumers would quite rightly object. Moreover, the term reinforces the worry that consumers, rather than being the primary beneficiaries of a "citizen-centric" identity management system, would be the primary product of a business-centric market.

[7] On the challenges of availability, affordability, and accessibility of ICT in Australia see for example Spiral Research and Consulting, *Another Barrier? Regional consumers, non-profit organisations, and the NBN in the Northern Rivers Region*, 4 July 2011, <https://accan.org.au/files/Reports/ACCAN_Anotherbarrier_WEB_V2.pdf>.

[8] The possible barriers caused by financial and access difficulties were raised in the public consultation for New Zealand's igovt service; see Gatt Consulting, *Public consultation about the igovt service: what people said*, prepared for the Department of Internal Affairs, NZ, March 2008, pages 30-34, <http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Identity-Verification-Service-Privacy-Impact-Assessments>.

Response to IIS's consultation questions

Do you understand how a digital identity services market could assist with increasing online trust?

There is clear benefit to consumers in increasing online trust, and in particular in helping to prevent online scams, frauds, phishing, etc. It remains to be seen whether the NTIF can provide such benefits beyond existing technologies. Existing technologies can, for example, authenticate a website using digital certificates in a way that is simple for end users to understand (through a coloured address bar or padlock icon, for example). While these methods are not fool-proof, in order for the NTIF to increase consumer trust a clear explanation of its improvements over existing technologies is needed. This explanation must be consumer-oriented; easier identification of consumers by government and business will not increase online trust for consumers.

At the same time, the possible risks to consumers must be acknowledged, and the steps taken to mitigate these risks explained. The current consultation round made several references to enhancing individual privacy, but the specific mechanisms by which privacy will be enhanced will need to be made clear in order for consumers to trust in the NTIF. Similarly, an explanation of how the system will avoid creating a "honey pot" of identifiable information will need to be provided.

More generally, the NTIF will better be able to increase consumer trust going forward as more detail is given. Further consultations should be conducted with increased input from civil society and the public generally to avoid creating the impression that the NTIF is being developed "behind closed doors".

Do you have a mental "picture" of a national market for trusted identity services? What are its key features? Who are the main actors?

From a consumer perspective, there are several key features of a NTIF:

- The NTIF should not merely be a means for government and business to better identify consumers (although this may offer some consumer benefit through reduced costs and data accuracy). Rather, the key benefits of the NTIF for consumers lie in improvements to a consumer's ability to identify organisations with which they conduct online transactions. It is therefore important that organisations' roles in the NTIF include their roles as users whose identity is to be verified, as well as their roles as identity and attribute providers and relying parties.

- Different types of organisation should provide identity and attribute information, depending on context. A social networking site may be best suited to providing identity information for casual online purposes; a bank may be best suited to providing identity information to financial institutions; and government may be best suited for providing core identity information (concerning, for example, passports and drivers' licenses).

- Privacy rights need to be strengthened through the NTIF. This includes making clear who is requesting and providing information, what information is being requested and provided, and providing the individual with the option to prevent the disclosure of the information.

Do you think the benefits of a national framework justify investment in it? What are the consequences of not having an NTIF?

It is difficult to answer these questions until more detail is provided about the NTIF. There will be costs and benefits in having the NTIF and costs and benefits in not having it, but until there is more detail there is no way of knowing whether the benefits justify the costs in either case.

Do you think there is a role for federal government in order to achieve a viable national market for safe and useable identity services?

Federal government must play a central role in the market. Consumers are likely to have greater trust and confidence in the government than in business, particularly when consumer sentiment is geared away from banks, telcos and credit providers (who, after government, are likely candidates for attribute and identity providers).

Government should ensure that the Framework protects and enhances the privacy of consumers and the security of information. The Framework should place limits on the provision and use of identity information in the identities market. Consumers are unlikely to have confidence in business (or even individual government agencies) to do this.

If so, what do you think is the best way for government to get involved?

- **facilitating the development of a national governance framework?**
- **stimulating either supply of or demand for digital identity services or both?**

Government's role (in addition to providing verification services on passports, drivers' licenses, etc.) should lie in both facilitating the development of the NTIF and in stimulating demand for identity services.

Which particular strategies for stimulating supply or demand do you think the government should focus on first? Should they do one or both?

The focus of government should be on stimulating demand in the identity market. If there is insufficient demand for identity services, then excess supply is likely to cause consumer concern at the needless provision of personal information into the market.

What identity services do you think government should continue to provide for the next 5 years versus long-term? For example,

- **should it continue as the authoritative source of identity data through birth certificates, passports, drivers' licences?**
- **should it continue to provide its own digital identity services such as social services cards, digital certificates for businesses, user accounts and passwords?**
- **should it continue to provide validation services for key identity documents, digital credentials and digital signatures?**

Consumer trust is more likely to rest with the government and authoritative identity sources (such as birth certificates, passports and drivers' licenses) than with private sector. It is important, however, that any government identity sources are not used where unnecessary.

Which of the three options for creating a market outlined in the paper do you think the government should adopt?

The government should pursue the "Enable Option". The "Encourage Option" and "Transform Option" would see the project proceeding too quickly, and without adequate time for assessments (including privacy impact assessments). Taking the time to assess the NTIF process is important both for building consumer trust and confidence and for ensuring that the NTIF project is successfully implemented. Failure to re-evaluate ICT projects over time has been noted as a reason for government ICT projects failing:

> If the project is approved, the business case 'becomes the core governance document for managing and measuring the project'. However, many business cases were not updated throughout their life. This was despite the projects continuing over several years or more, during which time assumptions, risks, costs, timelines and technology changed significantly.
>
> For example, the ICMS business case costs, timeframes and risks were based upon the assumption that a particular proprietary system would be used. However, the vendor responsible for that system did not bid for the project. The Department of Justice (DOJ) proceeded with a procurement decision and did not update its business case until after the 2009 VAGO audit. DOJ advised my office that it will re-consider the business case again after a review of ICMS has been completed.
>
> Good practice requires that the business case is:
>
> - reviewed at key decision points by the steering committee to ensure that the project remains desirable, viable and achievable
> - used as a benchmark against which to measure project performance
> - 'continually updated with current information on costs, risks and benefits'.[9]

[9] Victorian Ombudsman, *Own motion investigation into ICT-enabled projects*, November 2011, pages 26, <http://www.ombudsman.vic.gov.au/resources/documents/Investigation_into_ICT_enabled_projects_Nov_2011.pdf>.

What would the government need to do, at a minimum, to encourage private players to offer digital identity services?

- **Is it simply a matter of there not being clear standards around? If so, what particular standards are needed? For example, are standards needed for technical design, technologies, and business design to ensure interoperability, privacy, useability, and individual control?**
- **Or is it because there are no current private sector drivers (and thus government would need to go to market to stimulate change)?**

This question is best answered by private players. However, private players will be more likely to offer digital identity services if there is consumer demand for these services. This, once again, highlights the importance of building consumer confidence in the NTIF.

ACCAN also suggests that this question reflects a general focus on business concerns in the NTIF consultation process, and that future stages in the NTIF development should include a greater focus on encouraging consumer participation in NTIF identity services.