International Cooperation on Trust and Security Research:

An Australian Perspective

Malcolm Crompton
Managing Director
Information Integrity Solutions Pty Ltd

Presented at

Conference on

Trust in the Information Society

Session 5: International Cooperation on Trust and Security Research

León, Spain

10-11 February 2010

International Cooperation on Trust and Security Research: An Australian Perspective[1]

Some scene setting: What makes Trust, Security and Dependability such a challenging global issue

The theme of the conference is building trust in the information society. The RISEPTIS paper recognises that there is no 'magic bullet' for achieving this objective. Technology will be an important contributor but legal and enforcement frameworks in different jurisdictions will be just as important as well as individual expectations and capability, however influenced.

We cannot command trust from others: trust is a decision made by the other party. Instead, we can focus on establishing circumstances that might increase trustworthiness.

We are all aware of the challenges of establishing trustworthiness between parties within the European context. These challenges are magnified when seeking to establish trustworthiness between parties when both are not within the European context. If nothing else, the differences in cultural, political and market competitive structures will guarantee this.

The rapidly escalating economic power of Asia, from India through China, all the way round to Japan will only add to the challenge.

What next: Peering through the fog

Scenery like this suggests that new technologies and consumer expectations, driven by market forces and the fruits of research programs will be the fastest moving contributors to building trust in the information society and to establish trustworthiness with less effort.

However we are also seeing a stronger consensus emerge that this is less and less likely to be enough. It seems that there will be no avoiding a richer, multi-faceted approach.

At the official level, recent statements by Commissioner Reding as she transitions to become Member of the European Commission responsible for Justice and Home Affairs[2] clearly indicate that she recognises that the current regulatory protection of personal information in Europe needs updating. The same is emerging in the United States, for example the three Roundtables convened by the US Federal Trade Commission[3] and related speeches by its Chairman. Among the regulators, recognition that more is needed is also emerging, for example the Madrid Declaration[4] by the

[1] Please note that the observations and conclusions in this paper are those of the author alone. They do not purport to represent those of the Australian Government or any other government or any other organisation.

[2] See for example "Viviane Reding Member of the European Commission responsible for Information Society and Media Privacy: the challenges ahead for the European Union", Keynote Speech at the Data Protection Day 28 January 2010, European Parliament, Brussels online at http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/16&format=HTML&aged=0&language=EN&guiLanguage=en.

[3] Details available online at www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml.

[4] "International Standards on the Protection of Personal Data and Privacy", November 2009, online at www.privacyconference2009.org/media/Publicaciones/index-iden-idweb.html.

International Conference of Data Protection and Privacy Commissioners and the recent paper on "The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data" by the Article 29 Data Protection Working Party and Working Party on Police and Justice[5].

In the Asia Pacific region, the Data Privacy Subgroup is developing, brick by brick, an APEC cross border privacy rules system. The first components have already been endorsed by Ministers components.[6] This approach is looking specifically at how to improve trustworthiness in a cultural and regulatory environment that is so diverse it makes Europe look monocultural.

The OECD is also contributing to the thinking, facilitating a trans-Atlantic dialogue on strengthening accountability within and across jurisdictions as a major contributor to trustworthiness. The Data Protection Commissioner for Ireland facilitated the first part of this process. More recently CNIL, the French data protection regulator has been doing so.[7]

Can research and technology assist: an API for Privacy, Security or Trustworthiness?

At its simplest, an application programming interface (API) is an abstraction that provides an interface that can implemented by a software program to enable interaction with other software.

Moreover, as noted earlier, when it comes to establishing trustworthiness, we need to remember that it is not a binary state. A particular set of circumstances might increase or decrease trustworthiness, but only in extremes is it total or absolutely absent.

Unfortunately, this is too often forgotten in the thinking about trustworthiness outside the area that might be described as 'machine to machine' trustworthiness. Identity management is a particular case in point, especially in the case of identifying individuals. We might approach a binary 'trust or don't trust' state in tightly defined and relatively simple circumstances such as conducting a banking transaction. But this is unlikely ever to be the case across multiple domains and multiple jurisdictions.

A far better way of describing the challenge is to revert to the fundamental reason for developing trust, and hence seeking to establish trustworthiness. This fundamental reason is to reduce the risk in an interchange or a transaction, and to reduce the effort behind making the decision to trust, down to a level where the interchange is significantly facilitated or even goes ahead.

---

[5] The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data is available online at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp168_en.pdf.

[6] A good but dated summary of the state of play is online at www.dpmc.gov.au/privacy/apec/pathfinder_initiative.cfm. The final version of the APEC Privacy Framework was endorsed by APEC Ministers in 2005: http://apec.org/apec/news___media/2005_media_releases/161105_kor_minsapproveapecprivacyframewrk.html while the latest step has been the endorsement by Ministers of the APEC Cooperation Arrangement for Cross-Border Privacy Enforcement and associated documents in their 2009 Annual Statement, online at http://apec.org/apec/ministerial_statements/annual_ministerial/2009_21th_apec_ministerial.html.

[7] The first papers emerging from this project are online at www.hunton.com/Resources/Sites/general.aspx?id=690. There will be a further workshop in Paris in March to coincide with the OECD celebrations of the 30th Anniversary of the endorsement of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

In the highly heterogeneous world in which we live, in the short term there may be greater merit in finding something like an API for trustworthiness between individuals or between organisations, especially when they are in different jurisdictions, than in trying to force fit everything and everybody into the one framework. Given the heterogeneity of the trust decision process, this 'API' might indeed be a software API. In other cases, it is the API equivalent for a human to human or human to machine process but ideally the underlying metrics are the same or at least consistent.

If so, is the API for Privacy, Security or trustworthiness a risk rating for these parameters? Developing it would depend on agreement on what to measure, measuring it reliably, displaying it in a way that is easily understood.

Such a concept is hardly new: for years we have had credit risk rating schemas that rate the creditworthiness of organisations.[8] These ratings have been relied on so much that improved ratings can be worth many millions of Euros to an organisation in reducing its costs of borrowing. While ratings can also be manipulated, the system is a 'learning' system, so that for example the recent global financial crisis was both exacerbated by its failings but will also lead to its improvement.

But the key to the concept is 'caveat emptor': the ratings process attests to its process but not the result. The lender must make its own decision based on the information it can discover including the credit rating. The ratings agency must constantly improve its processes if it is to be utilised.

The possible application of this line of thinking to risk rating of an organisation's approach to privacy was outlined for the Privacy and Trust Partnership in Australia in 2007.[9]

Most importantly and like any good API, credit risk ratings allow for borrowing and lending across extremely diverse geography and jurisdictions. A privacy and security risk rating system has the potential to be the same.

Defining useable privacy and security ratings: a target for cooperation with Europe that could bring value for all?

Any ratings process must display a number of minimal characteristics to be useable. These include being:

- Objective in that different observers would reach a similar conclusion
- Measurable and quantifiable
- Resistant to gaming and manipulation

In addition, if they are to be taken up by the wider community rather than just a community of specialists and experts, they must also exhibit other characteristics including:

- Useable at the human level and/or
- Amenable to automation or computer aided implementation

[8] For the purposes of a paper like this, a wiki level description suffices. See for example http://en.wikipedia.org/wiki/Credit_rating_agency.

[9] The papers and a brief description of the project are online at: www.openforum.com.au/Privacy_and_Trust.

Again, there is the opportunity to draw on established practice in the world around us. For example, accessibility to ICT has something to teach us about better human-machine interface. For years, this steam of work has developed alternatives to small lettering on computer screens only capable of manipulation by well coordinated individuals using a keyboard. With the ageing population in many advanced economies, the proportion of the community that will expect better accessibility will increase dramatically. Moreover, this has great potential to make the information super-highway safe at greater speed through consistent design and predictability, just as it has for the real world highway.

We are seeing renewed interest in consistent and rapidly absorbed security and privacy information in the human-machine interface. Extended Validation Certificates and colour coding of the address bar in many web browsers is an recent example. Even more recently, initiatives on both sides of the Atlantic are emerging on consistent symbols to describe various privacy risks. In the US, the Future of Privacy Forum has recently launched the 'i' icon that it hopes will be added to most online advertisements that use demographics and behavioural data to tell consumers what is happening.

These kinds of initiatives have the great advantage of being able to cross language barriers and jurisdictions. However many of the initiatives to date have not gained widespread credibility for a number of reasons.

Thus development of trustworthy privacy and risk ratings and ways of communicating them to highly heterogeneous audiences could be a very valuable product of international cooperation.

Specific areas on the Australian agenda that could benefit from the European trust, security and dependability competencies

There are at least two significant areas where Australia could benefit from the European trust, security and dependability competencies.

These are:

- The development of the Australian National Broadband Network (NBN)[10]
- The development of eHealth first through the issuing of a single individual health identifier, then possibly a shared eHealth summary record (in addition to accelerating the exchange of eHealth information that will happen anyway) and concepts such as the digital hospital and coordinated chronic care.[11]

The NBN is a very ambitious project intended to provide 90 per cent 'fibre to the premises' coverage delivering speeds of 100 megabits per second with remaining coverage through state of the art wireless and satellite technologies at a slower speed. The project is anticipated to take eight years.

[10] For an official account of this initiative, see www.dbcde.gov.au/broadband/national_broadband_network.

[11] For an official account of national initiatives in eHealth, see www.health.gov.au/internet/main/publishing.nsf/Content/eHealth and www.health.gov.au/internet/main/publishing.nsf/Content/pacd-ehealth-consultation/$File/Typeset%20discussion%20paper%20-%20public%20release%20version%20070709.pdf.

At least a proportion of the network will be delivered by heterogeneous technologies and possibly even involve making use of underutilised and transient bandwidth. European input to managing the increased privacy and security risk from a significantly more potent network could be very fruitful.

With regard to the eHealth agenda, it would appear that there are eHealth initiatives in Europe that could be of significant assistance.

Australian national experiences that could aid and complement Europe's trust, security and dependability agenda

Australia, like many other parts of the world, does not have a single identity register delivered by government that is considered safe and reliable. Like any advanced economy, Australia has many 'sources of (some) truth' for authenticating many elements of an identity assertion. These include State (ie province) level registrars of births, deaths and marriages; a very well regarded passports issuing system that covers that part of the population that has travelled internationally; a very thorough Electoral Roll of those eligible to vote; State based driving licence systems; private sector banking systems, etc. The national health insurance scheme, Medicare, also has a very good record of details about most people living in Australia.

Nevertheless, Australia has needed to establish to acceptable levels the identity of individuals in other circumstances. One particular example is the policy of requiring anybody who uses financial services to be identified to an acceptable level of certainty commensurate with the risk associated with the transaction. This policy is established in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act).[12]

In other words, Australia has already established a risk rating approach to identity management in the financial services sector. It has a long established track record in this area going back to the 1980s, with the AML/CTF Act replacing earlier legislation simply requiring "100 points" of identification that was based on the production of a combination of source documents from a prescribed list of options.

Bringing it all together: Australia's experience with a risk based trust system

The Australian experience with a risk based approach to identity management could well provide a real world input to any cooperative research on a risk ratings approach to establishing trustworthiness.

That said, this is but one example of where cooperation between Australia and Europe would be beneficial. The 'information society' is increasingly borderless and the collective mind will be essential in making it a safe, respectful, enjoyable place to be.

[12] For a summary of the Customer Identification obligations of institutions under the Act, see www.austrac.gov.au/customer_id.html. For an example of the enforcement of this legislation, see "AUSTRAC accepts enforceable undertaking from PayPal Australia", Media Release dated 23 November 2009 online at: www.austrac.gov.au/23nov09.html.