A Possible Way Forward: Some Themes and an Initial Proposal for a Privacy and Trust Framework

A working paper for the
Privacy and Trust Partnership

Malcolm Crompton
Christine Cowper
Information Integrity Solutions Pty Ltd

Martin Abrams
Centre for Information Policy Leadership
Hunton & Williams LLP

PRIVACY&TRUST
PARTNERSHIP

November 2007

Table of Contents

A New Approach to Trust and Privacy in the Information Age

1. Introduction

1.1. The trust deficit

There is a world-wide trust deficit related to the use and protection of information in an information age. This deficit is reflected in the work of the Australian Law Reform Commission (ALRC) in Australia and the creation of the Privacy and Trust Partnership (P&TP). Even more interesting is that this trust deficit exists among individuals, business, regulators and government. Individuals often believe that the changes in business process that are made possible by information technology are not only not creating value for them, but make the market less user friendly. Business feels the current rules don't address the challenges they face and don't control the edge riders. Regulators believe that they don't have the resources to police an ever more complex marketplace. We have a system where there is a lack of faith that issues will be resolved, data will be under control, edge riders will be enforced against, and that the application of regulation will be predictable.

1.2. The P&TP Project

The P&TP is a consortium of businesses that have come together to think about the trust deficit (see section 4 below for more information about the P&TP and this project). It recognises that the trust deficit is an issue not only for business and is seeking to include individuals and other key stakeholders in its discussion. It also recognises that each of these parties will have its own interests and values and that a robust discussion will be needed if a viable solution is to be found. Early discussions have confirmed that there is indeed a range of perspectives and strongly held views that will be brought to bear on this issue. For example, business is looking for a system that vastly reduces complexity, while privacy and consumer advocates are concerned about losing hard won gains in privacy regulation, are wary about some of the claims that the current system is 'broken' and about assumptions that the value in personal information should unquestionably be released.

1.3. Scope including relationship to the ALRC inquiry

While this project has a longer term focus on the information economy and its key input – information about individuals – the ALRC work on privacy clearly has relevance here.[1] The proposition for this project is that there is a clear link between trust and maximising the potential benefits for business, individuals and government in the information economy. Information governance and the important subset of privacy are a critical part of the answer. The project both hopes to draw on the work of the ALRC and make a contribution to it.

[1] For more information about the ALRC inquiry see www.alrc.gov.au/inquiries/current/privacy/index.htm

The first step for this project as set out in the first White Paper[2] was to define the nature of the problem. The second step must be to define the objectives for a solution, and begin testing a hypothesis in the form of a possible framework for improvement. However, before we do that it is important to define the limitations of our process.

As we have said the territory for this project is information governance and the information economy. This intersects with the ALRC's privacy discussion but takes a narrower focus. Firstly, we think privacy protection can be broken down into three functional aspects:

- security;
- consumer protection;
- autonomy.

All three aspects are very important. However this project will focus on the first two. The third, autonomy – our ability to control others knowledge about us – requires a societal focus on how the individual relates to society as a whole that is beyond this paper. Autonomy can not be ignored. Indeed we believe the way we are dealing with the first two aspects may well feed into a discussion of the third.

Secondly, the project is not trying to solve all problems at once. This framework focuses on businesses wanting to do the right thing but will have beneficial flow on elsewhere in that (a) it will allow regulators to focus more of their scarce resources on malevolent or recalcitrant operators and (b) has the potential to raise the benchmark of individual expectations of government, with regard to government surveillance activities.

1.4. Possible outcomes and framework

We suggest the following possible objectives:

- less of the burden for policing the information environment falls on consumers and the actions they take based on being expected routinely to read notices and making choices based on those notices;
- consumers will nevertheless be able to exercise choice where it matters to them;
- consumers have confidence that they understand how to raise issues and that organisations will respond to those issues once raised;
- organisations using data analytics will understand the ground rules and have confidence that edge riders will be caught;
- health consumers will have confidence that health related information will be used appropriately and uses will be predictable;
- large organisations will be able to operate in a highly competitive market in a flexible manner with predictable regulation and enforcement; and
- new technology may be introduced with the confidence and knowledge that risks have been considered and there is a means for resolving new issues.

[2] Available online at www.openforum.com.au/Privacy_and_Trust

The paper then suggests one possible framework that may meet these objectives. The framework starts from the perspective that a set of privacy principles is necessary and that the framework should be established in law and should contain strong enforcement options. It places a new emphasis on how these elements work together. The framework recognises that implementation is as important as the underlying privacy principles. Implementation in turn must be able to demonstrate compliance with stated objectives, if it is to be credible. However, compliance does not convince until accountability processes are in place to demonstrate it externally. The final component that needs to be in place is an enforcement regime should all of these preceding elements not deliver. In short:

Implementation → Compliance → Accountability → Enforcement

The model aims to provide incentives for organisations to get privacy right, while being less prescriptive as to the how. The model is also intended to be responsive and dynamic; it can take account of changes in community views about practices that are intrusive, dangerous or sufficiently irritating.

Very importantly, this objective is achieved through the appropriate and transparent allocation of risk. It is likely that this risk allocation will lead to a transfer of risk away from the individual back onto the organisation, which apart from anything from anything else is usually in a better position to bear it. If nothing else, the more that risk allocation is opaque or is put onto the individual, the less trustworthy it is.

2. Themes for a framework for trust and privacy

2.1. Individuals need to be safe, able to trust and to be confident in the handling of personal information

The proposition in the first white paper was that an essential building block to an effective information economy is for individuals to feel 'safe'. And we argued that currently they do not feel safe. The first white paper put the view that a sense of safety will require more than reliance on variants of traditional principles and enforcement frameworks for the fair handling of personal information and suggested the extra dimension is trust.

Trust is an interesting issue for both organisations and individuals; they are not necessarily in the driving seat. Trust has to be earned and the only way to do this is by behaving in a trustworthy way. While acknowledging that individuals will have different expectations of trust and that trust means different things to people at different times, we suggest that from an organisation's perspective respecting privacy helps build trust and in turn that building trust will deepen relationships between individuals and organisation and lead to the willing exchange of personal information. Undoubtedly, there is commercial benefit possible here. However, it also seems likely an improved trust environment has the capacity to deepen relationships in other ways and to help individuals feel connected and part of society.

In thinking about trust, we suggest three key areas to address are: control; risk; and accountability.

2.1.1. Personal information under control

A central tenet in discussions about protecting individuals' personal information is 'control'. Control encompasses notions of autonomy, freedom from surveillance and ability to exercise choice. One approach here is the idea is that to be in control individuals must at least know who has their personal information and for what purposes and to the extent possible will be able to exercise choice.

Current privacy principles contain notice, use limitations and access provisions to promote individual control. While these provisions are and will remain important, it is arguable that they are less effective in practice than in theory, for example because of the sheer number of notices an individual would need to read and absorb, the observed tendency for individuals not to read or necessarily act on notices, and the practice of 'bundling consents'.

A better approach would be one where individuals have more 'real' control. This could be by better means of providing notice or by setting stricter rules. Another option would be to support notice/use limitation approaches by providing better mechanisms to assure individuals that their personal information is under control (while still allowing direct control where this is practicable and where individuals wish to exercise it) for example by:

- providing for adaptable information handling standards that could respond more specifically to culture and context;
- more robust transparency requirements for organisations;
- compliance audits published in certain circumstances; and/or
- risk/incentive frameworks to get information handling right.

2.1.2. Risk and accountability

Privacy risks arise when personal information about individuals is collected and used, for example to complete a transaction, make a purchase or make claim. The risks include the potential for personal information to be lost or misused, or used for unexpected or unwanted purposes. Consequences can be very harmful – from physical harm and financial harm to the chilling effects of feeling watched, manipulated or offended.

The question of risk in the handling of personal information, and who bears that risk currently receives little attention in general information handling statutes. The focus on giving individuals control – via notice and consent – has perhaps had an unintended consequence in that much of the risk is also given to individuals.

An added factor here is that there is generally no requirement for organisations to be accountable by providing assurance to individuals or to a regulator that they are taking the steps required by privacy laws. More often it is up to individuals or a regulator to take action if things go wrong. In effect individuals are being asked to be quite expert risk analysts and managers. The task involves at minimum examining privacy notices, understanding business processes and assessing security risks.

The relevance of risk in the privacy and trust context has probably increased as technology opens up new possibilities for business operating models. Moves from face to face services to call centres or other forms of remote contact including online have tended to also move more risk to individuals. They have to buy equipment and/or manage technical failures or losses through online security breaches.

The risk then compounds again. Too often organisations are also slow to accept responsibility quickly and effectively when failure occurs. While organisations manage their failures with business continuity plans, the equivalent is often missing for other stakeholders in a service provision relationship, especially the service user. Lack of a good safety net for service users when failure occurs is tantamount to allocating a disproportionate amount of risk to the individual, who is often least able to manage, mitigate or bear that risk compared with the service provider.

All this leads to one more issue: determining a fair allocation of risk. Should the fact that individuals have some input into deciding on level of risk, for example because they specify a particular communication channel, affect the allocation of risk.

2.2. Privacy principles essential

Privacy is accepted as an important and valuable element of Australian society and one that should be protected in law. Equally it is well recognised that privacy is an elusive concept and difficult to pin down, particularly when it comes to the task of regulation; in current schemes the process protections in information handling principles tend to act as a surrogate for the substantive or concrete privacy protections intended.

This paper, and the first white paper, suggests that some privacy principles are being asked to do too much work or are under performing. For example:

- it is impractical for individuals to give consent on a case by case basis for every usage of information in the Internet age;
- privacy notices are often unread and unreadable; and
- use limitation principles are challenging when new uses of previously collected information are contemplated and routinely have been circumvented by 'bundled consents'.

That said no obvious alternatives have previously presented themselves. In the longer term a tort of privacy, or a statutory cause of action for privacy, might take some of the role of privacy principles. In the absence of an alternative, privacy principles will continue to play a central role in any privacy and trust framework.

The question then is which principles? This question is currently the subject, amongst other things, of the current ALRC inquiry. Privacy principles have also been examined in the APEC privacy initiative.

Given the high level thinking that is already being done in those contexts, this paper is not attempting to also take on that task. The important point is that a set of privacy or information handling principles will be a necessary part of a privacy and trust framework.

2.3. Focus on outcomes not process

One of the contentions in the first white paper was that current information handling principles or standards are heavily process orientated and are not necessarily delivering on their intention of protecting individual privacy.

For individuals, process can also be onerous and is possibly ineffective. For example, there is a range of research suggesting that despite the wealth of privacy notices generated, people don't always read or understand them and may not act upon them.[3]

Process is also a cost for business, both in terms of direct compliance costs (preparing and providing notices) and opportunity costs. Some commentators also see regulatory rules that are, or are perceived to be, complex or restrictive, as hindering innovation in compliance approaches or business models. Dr Nicholas Gruen when commenting generally on the capacity for regulation to stifle innovation pays particular attention to privacy. The problem he identifies is the level of process and the way in which it drives organisation response:

> The finer points of much regulation – for instance, protections against spam, privacy, ensuring sufficient information is provided to consumers – make it virtually impossible to comply with the regulation by simply ensuring that one behaves commonsensically and with integrity and propriety.[4]

Performance based outcomes focussed approaches are well established in management theory and practice and in government administration. The Council of Australian Governments' 2004 best practice guide includes the requirement that:

> Regulation should have clearly identifiable outcomes and unless prescriptive requirements are unavoidable in order to ensure public safety in high-risk situations, performance-based requirements that specify outcomes rather than inputs or other prescriptive requirements should be used. This principle should also apply to any standards that might be referred to in regulation.[5]

For a privacy and trust framework a fairly fundamental question is what outcome are you looking for? This is not a small question. An almost universal point made in any discussion about privacy is that it is a difficult concept to pin down. Further, there are well respected privacy experts who argue that the subjective nature of privacy drives a procedural rather than a substantive regulatory response. This point is made for example in Bennett's and Raab's recent book on the governance of privacy.[6]

The point we are making here, while not claiming to be comprehensively argued, is that:

- a framework that allows for variation/innovation in process could bear fruit; and
- despite the difficulties, the effectiveness of a privacy framework may be tested better by asking, not have certain processes been met but rather are individuals actually well served, do they get "real" privacy rather than process.

[3] See for example, Robin McKenzie *Do people read privacy notices? New global work on improving the communication of important information about privacy practices - condensed (or highlights) notices:* Speech Privacy Contact Officers meeting, Canberra, 12 March 2004 at www.privacy.gov.au/news/speeches/sp3_04_files/frame.html; and Paul O'Shea and Dr Carmel Finn (2005) 16 Journal of Banking and Finance Law and Practice 5 Law Book Co,

[4] Dr Nicholas Gruen, Lateral Economics *Beyond Taylorism: Regulating for innovation Some ideas for discussion for the National Innovation Agenda* 28th August 2007 available at www.lateraleconomics.com.au/outputs/Beyond%20Taylorism%20-%20Regulating%20for%20Innovation.pdf

[5] Council of Australian Governments *Principles and Guidelines for National Standard Setting and Regulatory Action by Ministerial Councils and Standard-Setting Bodies* Amended by COAG June 2004, page 5 available at www.obpr.gov.au/publications/external/coag/coag.pdf

[6] Colin Bennet and Charles Raab 2006 *The Governance of Privacy Policy Instruments in Global Perspective* Cambridge Massachusetts the MIT Press

2.4. Less reliance on individuals "policing" their privacy

As we have noted above, today's privacy reality is that individuals are largely responsible for policing their own privacy (through notice, choice and access/correction rights). This 'front end loaded' model already expects individuals to spend extensive effort undertaking the tasks necessary. Even if they had the insight to do this well (and almost nobody does), it is highly inefficient.

2.5. Flexible, innovation-enabled environment for business

A key theme in the P&TP discussion is that modern businesses depend very much on information about individuals.[7] At the 4 July conference there was a clear sense that the business community recognised that trust and privacy were important elements in making higher and better use of information as well as a sense of frustration at the current rules. Issues mentioned included:

- the level of detail in the current frameworks which were seen as constraining and as forcing an overly legal response;
- the current system tended to close off uses of information that had not been anticipated when information was collected;
- notice and consent mechanisms are not necessarily effective control mechanisms and where overly broad or vey detailed may be damaging to trust relationships with individuals;
- a preference for clear rules about what was permitted and what was not.

These points, possibly other than the call for 'clear rules' could be seen to lead to a similar point to the outcomes discussion above.

The view coming through seems to be that this all results in a difficult and possibly conservative environment where business is driven by compliance needs and may be reluctant to innovate.

2.6. Law built on concept of responsive regulation

In Australia, individual privacy is protected by a range of laws. This paper is not re-considering the threshold question: law is needed. It sees a strong role for a legal framework for the protection of privacy and considers that any finetuning of the current system of laws is best considered in the ALRC's current inquiry into the Privacy Act; in fact the terms of reference for the inquiry contemplate this.[8]

The paper does suggest that the design of the legal framework and its application by a regulator should consider the principles of 'responsive regulation' which suggests answers

[7] A report on the conference and the main papers presented is available online at the Veda Advantage website and can be accessed at http://www.vedaadvantage.com/doc_library/55/PTP%20Congress%20Report%20Final%20Draft.pdf.

[8] The terms of reference for the ALRC inquiry into the *Privacy Act 1988* are available at www.alrc.gov.au/inquiries/current/privacy/terms.htm

to questions about how to regulate effectively and how to choose between regulatory tools that aim to either punish or persuade.[9]

In brief, responsive regulation:

- argues that regulation is more likely to achieve its goals where the regulator takes account of the regulatory environment including the nature of the industry or sector, the maturity of the regulatory regime, the size and complexity of the organisations to be regulated, and organisation and industry culture; [10]
- puts forward the 'regulatory pyramid' showing the hierarchy of tools available to a regulator and the extent to which they should be used. At the bottom of the pyramid are persuasive tools or strategies, including education, liaison or negotiated agreements which the model suggests should deal with the majority of cases. The smaller apex of the pyramid is reserved for the minority of cases where education and dialogue or investigations are unable to achieve appropriate change in practice earlier and include revocation of licence, sanctions or penalties depending on what the law provides;
- argues that effective regulation includes the capacity for escalation if cooperative, supportive and educative strategies fail; paradoxically the research shows that where the law provides for escalation to strong sanctions, and there is guaranteed commitment to use powers when necessary, in practice they are needed rarely.[11]

3. A possible framework for trust and privacy in the information age

The discussion below is one attempt to weave the themes identified above into a possible model. The model is intended to start the discussion. It is open to refinement or replacement should other models emerge.

The model is similar to current frameworks in that it starts with principles and includes a system of oversight and enforcement. The new element, which is intended to add power and flexibility to the system and which aims to support greater assurance for individuals and greater flexibility for business, is a system of privacy risk ratings for organisations based on their activities and how they go about their business, which then determines the applicable enforcement regime. The new framework would:

- allow an organisation to vary the principles by way of Binding Corporate Rules (BCR);

[9] J Healy and J Braithwaite, 'Designing safer health care through responsive regulation', *Medical Journal of Australia*, 184(10), 2006, S56-S59, p S56; J Braithwaite, 'Responsive regulation and developing economies', *World Development,* 34 (5), 2006, 884–898, p 887, quoted in Nils Baumgartner, Attorney-General's Department, '*Cooperation and Cross-Border Privacy Rules: building confidence in an accountable system for personal information moving between economies*' Background Paper Second Technical Assistance Seminar on International Implementation of the APEC Privacy Framework, 2007.

[10] J Braithwaite, J Healy and K Dwan, *The Governance of Health Safety and Quality*, Commonwealth of Australia, 2005, p 59 quoted as per note 8 above

[11] J Healy and J Braithwaite, 'Designing safer health care through responsive regulation', *Medical Journal of Australia*, 184(10), 2006, S56-S59, p S56.

- provide that where an organisation adopts approved BCRs it must also specify its approach to implementation, compliance and accountability – this might include new or traditional approaches to notice, Rolls Royce or Mini Minor security and so on;
- link adoption of BCRs to a requirement to undergo a privacy risk rating which would take account of the BCRs, the organisations' implementation/compliance/ accountability approach, and also taking account of the inherent privacy risk in the proposed use of personal information based on issues of concern to the community; and
- set the enforcement framework, for example, external accountability obligations and level of penalties, based on the organisation's risk rating.

The system intends to encourage organisations to aim for low risk ratings; for example by finding ways to make its activities less risky (for example by using de-identified information) or by adopting more stringent security, accountability and safety net or other measures.

3.1. Privacy Principles: a benchmark against which variations are possible

In the proposed framework, privacy principles would remain the benchmark. The paper suggests the Unified Privacy Principles (privacy principles), as proposed in the ALRC discussion paper as the starting point.[12]

Organisations would then be able to vary the principles for their own circumstances – that is to draft BCRs to replace the default privacy principles that combined with their approach to implementation would then be subject to a compliance and enforcement framework appropriate to those decisions.

The proposal is similar to the privacy codes option contained in the private sector provisions of the Privacy Act.[13] As in the Privacy Act, this framework would require that variations to the privacy principles would be subject to external approval, at the minimum by the Privacy Commissioner. Any variations in the principles that might be perceived as a weakening would need to be compensated for by the variations in other principles and by the surrounding compliance, accountability and enforcement framework.

A challenge would be to make sure that the potential variation in principles from organisation to organisation or between sectors does not disadvantage individuals. Under the model proposed here, the intention would be that an organisation's approach to implementation, compliance and accountability as well as the surrounding enforcement framework would respond to the nature of the privacy principles adopted and the inherent risk involved in an organisation's activities. The aim is for stronger protection for individuals and stronger incentives to encourage organisations to do the right thing – all part of ensuring that the organisation bears an appropriate proportion of the risk involved rather than shifting it onto the individual.

[12] See section 15 of the ALRC discussion paper at www.austlii.edu.au/au/other/alrc/publications/dp/72/27.pdf

[13] See Part IIIAA of the Privacy Act and the views of the Privacy Commissioner set out in "Getting in on the Act: The Review of the Private Sector Provisions of the *Privacy Act 1988*", May 2005, available at www.privacy.gov.au/act/review

3.2. Emphasis on assurance measure including audits

A feature of the framework proposed is its intention to build in a new attention to assurance and accountability. One of the key mechanisms here is likely to be a move to much more extensive focus on applying assurance programs to privacy practices, be it through audit or otherwise. Under the current frameworks assurance processes tend to fall to the regulator or to the individual. There are exceptions of course; some sectors, and particular larger companies, already undertake compliance audits.

The proposal here is to encourage routine and widespread assurance processes. It is unlikely that any regulator would have the resources to take on the work involved. Practically then much of the assurance process would be undertaken at the organisation's expense and drawing on private sector expertise. The regulator would continue to take a strong role but would be freed up to focus dealing with the recalcitrant and the edge rider, monitoring the system as a whole and dealing with new issues.

The proposed assurance process would be very similar to the current requirements for organisations to undergo such procedures for their financial information. It should also be noted that in Australia at least the credit reporting sector and organisations that are tax file number recipients are already subject to audits. This new assurance process would replace some of the regulatory work in relation to privacy that is currently undertaken by the Privacy Commissioner and hence funded by the tax payer.

3.3. Implementation, compliance and accountability: additional flexibility to innovate

In order to take advantage of the option to tailor privacy principles organisations would need to be open and up-front about how they intend to go about meeting the requirements of the privacy principles. There are clear opportunities here for organisations to innovate and to demonstrate their points of difference to their customers.

3.3.1. Implementation

An organisation's implementation approach would need to be sufficiently detailed to feed into a realistic risk rating. It might cover matters such as:

- the steps an organisation would take to implement the relevant privacy principles or BCRs, for example the strength of a public awareness campaign that might be in place instead of an individual notice principle or the form of access offered and the access process; or
- the proposed safety net including any membership of an alternative dispute resolution body.

3.3.2. Compliance

An organisation's risk rating would also be affected by the compliance regime that it proposes to work under; that is how it will go about meeting the obligations in its BCR. This might include matters such as:

- how it will manage privacy, including who is responsible and complaint handling approaches;
- how it will identify and document its information handling processes;
- its approach to staff awareness and training;
- the nature and frequency of its internal and or external assurance process, such as audits etc; and
- its history of misdemeanours, which might include:
  - failure to maintain security levels;
  - failure to obtain a risk assessment;
  - failure to seek audits or to publish the results if required.

3.3.3. Accountability

For the purposes of the framework, accountability is essentially the means by which organisations are held to account. Accountability measures could include transparency (publishing audits, complaints statistics etc) and response to external parties (for example in the course of complaint investigations). Accountability approaches might also address an organisation's:

- approach to privacy breaches, including if/when it might notify individuals about any breaches;
- whether the result of any assurance processes are published, and/or if they are provided to the regulator; and
- participation in a respected complaints handling process that meets recognised standards of independence and capability[14]

3.4. Privacy risk rating model: assessing an organisation's approach to privacy

The proposed risk rating system needs to be both simple and robust. Preferably, it should also be recognisable from regulatory frameworks in existence elsewhere that have been well tested over many year; possible models include the credit rating of companies by credit rating agencies such as provided by Standard and Poors or Moody's and from the governance and compliance framework that has grown around financial information. Indeed, the latter recognises that over time a likely path for information governance is that the elements of information holdings commonly seen in organisations such as financial

[14] See for example those that are required of code complaint handling processes as spelt out in the Regulations to the Privacy Act, online at www.privacy.gov.au/act/Regulations/index.html

information, personal information, intellectual property etc will be drawn together into an integrated, risk based governance and compliance framework.

A number of components in such a framework would need to be developed and these are outlined here. The descriptions are not complete, but should be sufficient to allow debate between stakeholders on the merits of the model and which options to choose in refining its design.

3.4.1. Voluntary or mandatory risk rating for organisations

As with any change or innovation, it is important to consider how to introduce the privacy risk rating system. Options include making it voluntary, targeted or applied to all organisations. For example, there might be a two tier system such as the following:

- the first tier would be the 'default' position in which organisations handling personal information would have to comply with the benchmark privacy principles, would be the subject of investigations and possibly audit by the regulator and in addition, if things go wrong, they would be subject to a strong system of sanctions, including fines, restitution to individuals affected and long term assurance programs such as those that have been imposed by US regulators, lasting sometimes for decades; and
- the second tier would be made up of organisations choosing the BCR and risk rating route and would be subject to a regime of sanctions and enforcement obligations based on their risk.

A privacy risk rating process could be implemented in a number of ways. The aim would be to have a simple process, that would leverage off other processes where possible and that would be at a level of cost and intensity to match an organisation's business operations and size. The options would include risk rating by a regulator, or by organisations accredited by a regulator, or by a published self assessment.

3.4.2. Construction of the risk rating

There are likely to be a number of ways to proceed in constructing the privacy risk rating; regardless of the way chosen, the design of the privacy risk rating methodology is likely to be very challenging in part because it would need to be able to evolve in response to changing circumstances. For the purposes of discussion the paper sets out below one possible set of elements for a risk rating.

3.4.2.1. Privacy principles

The idea would be to start with the UPPs or if adopted an organisation's BCRs. Strengthening or weakening of the principles by way of the BCRs would affect the rating of that principle. So, a change to a principle to require consent for any new use of information may reduce the risk associated with the 'use' principle by a few points while a change in the 'collection' principle to rely on general rather than specific notice may increase the risk by a few points. Organisations would have an incentive to improve on the benchmark principles.

3.4.2.2. Implementation approach

The second component of the risk rating would depend on the organisation's approach to implementation, compliance and accountability. The rating might be applied to key elements in implementation such as complaint handling, membership of an alternative dispute resolution scheme or identity management or security, and the strength of its compliance program (self assessment or external assurance etc) and how it reports in normal circumstances to the wider world. Strengthening or weakening of an element would increase or decrease the rating.

The framework proposes that the 'Safety net' for individuals would be a significant element of this second component – to gain a privacy risk assessment the process must spell out the safety net it offers to individuals when a breach of privacy is suspected or discovered.

3.4.2.3. Inherent privacy risks in proposed use

The third component of the rating would bring in a factor for the inherent riskiness of the proposed use of personal information. This aspect of the rating might take into account industry sector and the nature of personal information held, for example whether it related to an individual's health or financial affairs. It would also need to be responsive to changes in community attitudes to uses of personal information.

If the system cannot do this, if it cannot head off practices that people find damaging, intrusive or sufficiently irritating, trust will continue to be undermined and probably inevitably more legislation will follow. Community attitudes surveys undertaken by the Privacy Commissioner or others could be one way in which the perspective of the consumer could be injected. Should Australia or any Australian state introduce a tort of privacy, or a statutory cause of action for invasion of privacy, court decisions that follow could also feed into the risk rating.

3.4.3. Risk rating model in summary

The discussion above can be represented by the formula below. This representation is intended to give another perspective on the model but one possibility would be to build the model so that it did produce a numerical risk rating.

Privacy Risk Rating = [Inherent Use Risk] x [$\sum$ Principle Ratings] x [Implementation/compliance/accountability approach].

0 = low	0 = strong	0 = strong
2 = high	25 = weak	2 = weak

3.4.4. The privacy risk rating process

There are many options for establishing the decision making process but it should be one that allows the approach or formula to develop as technology develops, community expectations change and business responses develop. It would also need to be widely respected in the community as fair and effective.

The best outcome would be to have maximum flexibility consistent with trustworthiness. The path to achieve this would probably change over time. In the start up phase it may be that the legislative framework would be quite prescriptive. It may also include a regular review process that could look at the work of the august body, and the way the framework as a whole is working. Over time it is likely that the system would become less prescriptive and the august body would have more autonomy in the matters considered, the settings and so on.

3.5. Enforcement: the stick behind the carrots in the legal framework including sanctions and restitution for individuals

The law always operates in the context of economic activity – the market place. It is therefore no surprise that with the establishment of a privacy risk rating system such as has been described here, participating organisations would face two types of incentive to lower their privacy risk rating.

The first would be market forces. Competitors with a lower privacy risk rating could be expected to use it to achieve a market advantage.

However history has also shown that market forces, while helpful, are not always sufficient to achieve standards expected by the community, whether it be motor car safety or fuel economy, toy safety, general consumer protection or many other examples.

Hence, in line with the discussion above this paper proposes that this privacy risk rating system would be firmly established by law. The paper is not seeking to lay out a detailed legislative scheme. It provides a flavour of a possible legal framework to assist the discussion.

The paper proposes three key safeguards which it considers would provide the bedrock on which the more flexible aspects of the framework could be grounded and contribute to building a stronger responsive regulation framework.

3.5.1.1. Penalties for prima facie 'bad behaviour'

In discussions with stakeholders at the 4 July conference and afterwards it was suggested that it would be valuable build in a process to identify any information handling behaviour by organisations that might be considered 'prima facie' to be so inconsistent with community expectations of privacy that it should be stopped. A number of participants suggested the *Trade Practices Act 1974* concept of 'unconscionable conduct' as possible model.

The inclusion of the concept of 'unconscionable privacy behaviour' and the tools for the regulator to take action could have strong benefits in terms of clarifying acceptable standards of information handling and acting as one of the 'sticks' that while not necessarily used much appear to be necessary for effective, responsive regulation.

3.5.1.2. System incentives including fines and penalties for compliance breaches

A key feature of the incentive approach being proposed here is to make sure that the fines and penalties reflect each organisation's privacy risk rating. This could again take a number of approaches. Only one is provided here by way of example, as follows.

Where an organisation is operating with a high risk rating (which would mean either high inherent risks, or a high risk implementation approach) this rating would in turn apply to the penalty points attaching to a provision. For example, the number of penalty points could be multiplied by a fraction of the privacy risk rating so that fines rise steeply with the rating. This fraction is a factor that could be adjusted in light of experience to produce the right level of incentive.

The enforcement system should also recognise that organisations will occasionally fail despite best endeavours and that, except where behaviour is egregious or repeated, the system should encourage such failures to be dealt with in a low key but highly responsive way rather than immediately bringing down the full force of the law. The idea is to have a range of power, tools and penalties to deal with failures without necessarily expecting that these would be used frequently.

The system of penalties and incentives might attach to:

- failure to meet the standards and expectations created in the BCRs and associated implementation/compliance/accountability arrangements established by the business that led to its privacy risk rating;
- failure to maintain security levels;
- failure to obtain a risk assessment;
- failure to seek audits or to publish the results if required;
- failure to provide a complaints handling service commensurate with the arrangements put in place as part of the compliance and accountability arrangements established by the business that led to its privacy risk rating;
- unconscionable privacy conduct;
- security breaches and here may also include requirements to notify individuals affected by the breaches in certain circumstances.

3.6. Strong regulation, assertive harms focussed regulator

A key plank in the framework is the need for a strong assertive regulator. The importance of such a role is emphasised in the responsive regulation approach (at section 2.6 above), by writers such as Bennett and Raab and in the ALRC report which recommends increasing both the powers and flexibility to decide on courses action, for the Privacy Commissioner.[15]

In this framework, which intends to build in high levels of incentives to protect privacy and build trust and high levels of accountability and transparency throughout the system, the regulator's role would be to both have a deep and strategic understanding of how the framework was working and the readiness to take effective, and strong action where issues or difficulties were emerging.

[15] "The Governance of Privacy", by Colin J. Bennett and Charles D. Raab, MIT Press, Feb 2007; for a comprehensive book review, see www.bsos.umd.edu/gvpt/lpbr/subpages/reviews/bennett-raab0207.htm

[15] See "Powers of the Office of the Privacy Commissioner", section 44 of the ALRC discussion paper, at www.austlii.edu.au/au/other/alrc/publications/dp/72/27.pdf

3.7. Safety net for individuals

A number of the strands of the discussion above are intended to build an effective safe net for individuals; for example the framework considers the fair allocation of risk in transactions and encouraging organisations to consider broad and practical means to mitigate that risk. However, there will be cases where these measures are not sufficient and a process for restitution needs to be pursued.

The current framework appears to provide an appropriate model here: individuals have a right to complain but generally speaking only after they have attempted to resolve the issue with the organisation concerned. The risk rating framework would also be an incentive to organisations to sort out individual's issues as quickly as possible. A further incentive to ensure that complaints resolved at the earliest level possible would be to provide that complaints that were escalated to the Privacy Commissioner would attract a charge payable by the organisation.

4. Concluding remarks – where next

This paper sets out a perspective on the challenge to privacy protection as currently constructed and the greater challenges that it faces in the future. It also sets out a possible framework for addressing those challenges.

The next step is to debate these proposals in order to develop something even better.

5. About the Privacy & Trust Partnership and this project

The P&TP is a consortium of businesses that are very much part of the information age, whose core activities rely on personal information. The Consortium members are Veda Advantage Limited, Acxiom, IBM, SAS, Suncorp and Microsoft. The consortium is funding a project which is intended to:

- foster a robust and sustained discussion about the impact of the revolutionary change in information management on privacy;
- develop an approach that facilitates respect for consumer privacy, earns trust and protects from harm and that creates economic value for everybody.

The consortium has asked Information Integrity Solutions Pty Ltd (IIS) and the Centre for Information Policy Leadership (CIPL) to assist it to foster a robust discussion between interested parties including business, relevant areas of government and privacy and consumer advocates. IIS and CIPL are consultancy firms specialising in privacy and based in Australia and the United States respectively. More information about the firms is available at:

- www.iispartners.com
- www.hunton.com/Resources/Sites/general.aspx?id=45

The steps in the project are set out below.

5.1.1.1. First white paper and 4 July 2007conference

The first white paper A New Approach to Trust and Privacy in the Information Age, by Malcolm Crompton, Marty Abrams and Chris Cowper is available at:

- www.openforum.com.au/Privacy_and_Trust; or
- www.iispartners.com/white_paper.pdf.

The paper is intended encourage this discussion by starting to identify themes and possible frameworks for thinking about privacy and trust in the information age. The report of the conference is available at:

- http://www.vedaadvantage.com/doc_library/55/PTP%20Congress%20Report%20Final%20Draft.pdf.

5.1.1.2. Working paper and 4 December 2007 workshop

The first white paper set out to define the nature of the problem. This working paper focuses on the second step which is to refine the objectives for a solution, and begin testing a hypothesis for improvement. It will be the subject of a discussion with invited participants at a workshop in Sydney on 4 December 2007. The group will consider the possible framework set out in this paper, identify and explore issues. IIS and CIPL are essentially seeking feedback on whether it is fruitful to pursue these directions and on areas for further development.

5.1.1.3. Next steps

The current intention is that IIS and CIPL will develop the ideas in this paper into a second white paper for the P&TP. It is also expected that a further conference will be held in the first half of next year.