

# *A New Approach to Trust and Privacy in the Information Age*

A 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

July 2007

---

## Table of Contents

|           |  |           |
|-----------|--|-----------|
| <b>1.</b> | <b>INTRODUCTION.....</b>                                   | <b>3</b>  |
| 1.1.      | WHY THE PROJECT .....                                      | 3         |
| 1.2.      | SCOPE AND CONTEXT FOR THE PAPER .....                      | 3         |
| <b>2.</b> | <b>WHAT'S THE PROBLEM .....</b>                            | <b>4</b>  |
| 2.1.      | INDIVIDUALS DON'T FEEL SAFE.....                           | 5         |
| 2.2.      | BUSINESSES FIND PRIVACY LAW UNPREDICTABLE.....             | 6         |
| 2.3.      | INFORMATION ECONOMY INPUTS AT RISK .....                   | 7         |
| 2.4.      | REGULATOR FRUSTRATION .....                                | 8         |
| <b>3.</b> | <b>HOW DID WE GET HERE .....</b>                           | <b>9</b>  |
| 3.1.      | INFORMATION STORES NOW AND 40 YEARS AGO .....              | 9         |
| 3.2.      | THE 'RULES OF THE GAME' AS THEY ARE TODAY .....            | 9         |
| 3.3.      | BURDEN OF NOTICE AND CONSENT .....                         | 10        |
| 3.4.      | DISCONNECT BETWEEN BUSINESS VIEW AND INDIVIDUAL VIEW ..... | 11        |
| 3.5.      | DEVELOPMENT OF THE LAW IN FITS AND STARTS .....            | 11        |
| <b>4.</b> | <b>ECONOMIC VALUE OF DOING BETTER.....</b>                 | <b>12</b> |
| <b>5.</b> | <b>STAKEHOLDERS - WHAT DO THEY NEED .....</b>              | <b>13</b> |
| 5.1.      | INDIVIDUALS .....  | 13        |
| 5.2.      | BUSINESS.....  | 14        |
| 5.3.      | GOVERNMENT.....  | 14        |
| 5.4.      | REGULATOR .....  | 15        |
| <b>6.</b> | <b>FORETELLING AND CHALLENGE FOR FUTURE.....</b>           | <b>15</b> |
| <b>7.</b> | <b>CONCLUSION.....</b>                                     | <b>16</b> |

---

# A New Approach to Trust and Privacy in the Information Age

## 1. Introduction

### 1.1. Why the project

The quest to design a new approach to trust and privacy in the information age is a high stake enterprise; one that if successful will release enormous further economic value in personal information and make the society one we want to live in.

Almost all western democracies have frameworks for the protection of personal information, including in privacy laws. However, there is a general feeling of unease; a feeling that these frameworks are either breaking or broken. Traditional privacy protection is based on the notion of giving individuals fine grained control and expecting them to want and be able to exercise it. Arguably the current laws do not deliver well on this objective; nor do they give individuals confidence or trust in the information handlers. Is this a question of compliance or a more fundamental design issue?

The right approach to trust and privacy is not just an issue for Australia. It is a global issue eventually requiring a global response. The importance of getting the privacy framework right is well recognised in many countries and in forums such as the European Union (EU), the Organisation for Economic Cooperation and Development (OECD) and the Asia-Pacific Economic Cooperation (APEC). Unfortunately, there is real potential for the efforts on all these fronts to turn into a process nightmare of questionable efficacy, especially if legislative change is an emergency response to a new development in technology, a new business practice or otherwise.

What is needed is some new thinking that delivers both better privacy and more efficient business practices, not with more rules and restrictions but with a greater understanding of what is needed for real trust to exist between individuals and business that when personal information is revealed there will be no surprises in how it is handled and if things go wrong there will be swift and efficient restitution. At best, innovation by business, perhaps in the form of new business processes or deeper use of probalistics, or by individuals, as we see emerging in the world of 'Web 2.0', should be able to develop safely with minimal hindrance.

This paper provides some initial thoughts for a group, unique in the depths of its interests, that will come together to do some thinking about the issues. If we don't pay attention to the problem we will continue to face economic damage, lives that are damaged and emergency response to shock; including more regulation and other inefficient attempts to deal with the problems as they arise. Even in Australia where we have a Privacy Act, we now also have the *SPAM Act 2003* and the *Do Not Call Register Act 2006*. These pieces of law are not always consistent and come with compliance costs. The question arises is this the best way of doing things?

### 1.2. Scope and context for the paper

The aim of this paper is to put forward the starting ideas for a unique discussion between stakeholders, government, regulators, industry and consumers about the possibility of a better approach to privacy regulation. The paper does not purport to present iron-clad evidence for its propositions. Nor does it propose to present solutions. It lays out the issues, as seen by some who have been working in the field for many years. If the conclusion that the current privacy framework has reached its use-by date is right, then no less than a paradigm shift is needed to move forward.

This is not to suggest that every element of the current regulatory framework needs to go. For example, it is hard to imagine a regulatory framework without standards or principles for the collection, use and disclosure of personal information. While beyond the scope of this paper, part of the thinking process would be to retest current privacy principles in any new paradigm and framework.

The aim in starting this discussion is not necessarily to achieve immediate consensus or even make specific proposals. Rather, the aim is to build a new capacity for consideration of key issues in trust, privacy and the information economy which can then be taken forward in other forums.

This paper is intentionally focussing on the interactions between individuals and business. It is here that there is immense potential value creation in the use and networking of personal information. However, a test of any framework for the regulation of privacy and personal information will be whether it can also translate to the public sector, or can work seamlessly with that sector. This has moved from the realm of the desirable to the realm of the essential as the boundaries between government and the world around it have blurred first through outsourcing and private provision of previously public services, increased co-production in law enforcement such as in the taxation and anti-money laundering arenas and in the future as 'Government 2.0' emerges.

The paper and the subsequent dialogue that it is intended to facilitate is also being prepared in parallel to a thorough-going review of the *Privacy Act 1988* (Cth) by the Australian Law Reform Commission (ALRC). The ALRC will report in 2008.<sup>1</sup> This paper looks beyond that inquiry in that:

- it is looking to the privacy regulatory framework that might be in place in 5-10 years;
- its particular focus is on the data governance needed to deliver the consumer trust necessary to maximise the value creation in the use and networking of personal information;
- it has a primary focus on the private sector.

To help frame the discussion this paper will firstly set out some of the evidence pointing to the proposition that that the current framework may be breaking or broken. It will then give a perspective on factors leading to and compounding the problem. The paper will then take an initial look at the economic impacts of the current system. It will then put forward a few thoughts on where a better future might lie.

## 2. What's the problem

As members of the Australian society we all play multiple roles. We are employees and family members. As citizens we vote, use public services, buy goods and services in person or on-line, belong to clubs and communicate with our friends and families. Increasingly, these interactions leave a paper or electronic trail that may be collected in the context of one role and transferred to another. However, every society allows individuals to have some space where they can define themselves rather than being defined or even act anonymously. In some instances, there is not only a strong private interest in these freedoms but there is also a strong public interest as well. For example, the freedom to read without having what we read being monitored, except perhaps in the most extreme circumstances, is an essential pre-requisite to a democracy.

Unquestionably some transactions, for example where there is a debt to be paid, do rely on the parties being identified, opening up the possibility of collection and re-use of the trail generated. Again, this

---

<sup>1</sup> For more information on the ALRC's privacy inquiry see [www.alrc.gov.au](http://www.alrc.gov.au)

is in no way saying there should not be a space where individuals can be free of an information trail, including being anonymous if they wish and if permitted by the society.

Our ability to collect, process and share information has revolutionised business processes, from the delivery of parcels to the development of new medical therapies. We use information to make decisions, manage risk, perfect addresses, chart the relationship between disease and genetics, provide service 24/7, team individuals to solve problems and create teams without moving individuals from place to place. Clearly the process of releasing the value in personal information is well under way. However, the continuing huge yearly increase in the creation of data (see discussion on 'How did we get here' below) and the predictions of business analysts such as Bruce McCabe, suggest that we have hardly started and that there is much more upside to be released.<sup>2</sup>

A possible brake on the release of value is the package of law aimed at protecting privacy and which some in business find is costly, restrictive or both. This is not to say that the business community does not see value in privacy and particularly in keep personal information secure. After all information is now a key asset for many businesses. Rather the concern is with the current protection framework.

Equally, it appears the current package of laws is not delivering for individuals, meaning they are less willing to cooperate with the value release project.

If the regulation framework is not thought through, the risk is an ever increasing mess of inconsistent law. This section of the paper will explore some of these issues and some of the evidence for them.

## **2.1. Individuals don't feel safe**

In short, many individual consumers feel uneasy: apathetic, doubtful or concerned. They think they are ineffective in having an impact on a world that has a depth of knowledge about them. They report that they don't really know what is going to happen to their personal information. Unanticipated uses of information are becoming a huge trust conflator. Individuals are distrustful and take what steps they can, including: withdrawing from services; falsifying information; or calling for more law.

Research is showing that individuals worry about loss of control over their personal information whether they are dealing with government agencies or the private sector. This could be loss of control they themselves might have over it, or loss of control by the people or entities to which they have given their personal information.

In turn, this concern appears to be driven by uncertainty about whether or not individuals can trust the entities to whom they give personal information, or who have control over it, to look after it and use it appropriately.<sup>3</sup>

---

<sup>2</sup> McCabe, Bruce *The Future of Business Analytics* S2 Intelligence available at [www.s2intelligence.com.au](http://www.s2intelligence.com.au)

<sup>3</sup> See eg Malcolm Crompton papers "The Trust Cluster: Dealing Effectively with Security, Privacy, Identity and Authentication at the Heart of Connected Government"; and "Respecting people, their individuality and their personal information: The Key to Connected Government, now and in the future", online at [www.tispartners.com/publications.html](http://www.tispartners.com/publications.html) and [www.cisco.com/web/learning/le21/le34/nobel/2005/post/presentations.html](http://www.cisco.com/web/learning/le21/le34/nobel/2005/post/presentations.html)

Research is also showing that whether individuals are prepared to trust an entity often depends on the risks of failure of any sort and who bears that risk when it comes to pass.<sup>4</sup> This research is supported by an increasing array of surveys canvassing individuals' attitudes to privacy. For example the 2004 Yankelovich report found that

It comes as no surprise that consumers today report having very little trust in institutions generally, and corporations in particular. Just how low is trust? The data suggest that anywhere from two-thirds to four fifths of Americans display a profound distrust of institutions.<sup>5</sup>

Privacy and consumer advocates, who generally are in a position to take a broader, systemic view of things, are also dissatisfied with current levels of privacy protection. They tend to see the problem as insufficient law and/or insufficient enforcement. For example, the Australian Privacy Foundation's (APF) submission to the ALRC Privacy Inquiry called for changes to the privacy principles to:

- require more details about disclosure, for example if asked to identify specific organisation to whom personal information is disclosed;
- prefer direct rather than indirect collection;
- impose more limitation on onward disclosures; and to
- strengthen anonymity/pseudonymity.<sup>6</sup>

The APF also called both for the regulator to take a tougher regulation stance, including greater use of powers to conduct audit and to make determinations in relation to privacy complaints. Interestingly, the advocate community in Canada put forward similar comments to the Committee reviewing the Canadian private sector privacy law.<sup>7</sup>

Whether the answer is more, stronger law or something else, the consequence in losing individual trust was clearly put by Google CEO Eric Schmidt on 20 June 2007. Schmidt, talking about the possibility of users deserting Google's services, noted that "If people stop trusting Google, then we have a problem. Everything is gated on this issue. Our rivals are only one click away".<sup>8</sup>

## 2.2. Businesses find privacy law unpredictable

For business information represents potential value; value may come from the initial use or in using information in new contexts. Limits on use, whether because of legislation or consumer resistance, may curtail innovation, limit outsourcing choices or the future use of historical data in new contexts. Decision-making in this unpredictable environment becomes difficult attracting risks to reputation where consumers do not trust a proposed or unexpected use of data; and regulatory risk where there is a knee jerk regulatory response to a problem that flares up in the public eye.

Business has found ways to work within existing privacy law. But the question is whether or not that law works optimally to achieve the potential value creation in the information economy.

At one level, the business sector reports comfort with the current privacy law. For example, on the basis of submissions to the review of the private sector provisions of the Privacy Act the Privacy Commissioner reported that "the overall view from the business sector is that the scheme [private

---

<sup>4</sup> See "Trustguide Final Report", October 2006, UK DTI et al, online at [www.trustguide.org.uk](http://www.trustguide.org.uk)

<sup>5</sup> YANKELOVICH, Re-building the bonds of trust: state of consumer trust, crisis of confidence Presented to: 10th Annual Fred Newell Customer Relationship Management Conference 2004 available at [www.compad.com.au/cms/prinfluences/workstation/upFiles/955316.State\\_of\\_Consumer\\_Trust\\_Report\\_-\\_Final\\_for\\_Distribution.pdf](http://www.compad.com.au/cms/prinfluences/workstation/upFiles/955316.State_of_Consumer_Trust_Report_-_Final_for_Distribution.pdf)

<sup>6</sup> Australian Privacy Foundation submission to the Australian Law Reform Commission Review of Privacy Issues Paper 31 January 2007 available at [www.alrc.gov.au/inquiries/current/privacy/index.htm](http://www.alrc.gov.au/inquiries/current/privacy/index.htm)

<sup>7</sup> See transcripts of the committee inquiry at [http://cmtc.parl.gc.ca/cmtc/CommitteeHome.aspx?Lang=1&PARLSES=391&JNT=0&SELID=e1\\_COM=0](http://cmtc.parl.gc.ca/cmtc/CommitteeHome.aspx?Lang=1&PARLSES=391&JNT=0&SELID=e1_COM=0)

<sup>8</sup> See [www.pcpro.co.uk/news/115959/googles-schmidt-talks-trust-and-privacy.html](http://www.pcpro.co.uk/news/115959/googles-schmidt-talks-trust-and-privacy.html)

sector provisions of the privacy Act] has worked well for them, and that there is considerable support for it as it currently stands".<sup>9</sup>

Possibly, the sentiment being reflected here is that business can work with the law, rather than finding the law works optimally.<sup>10</sup> Add in the prescriptive and complex provisions of the Privacy Act's credit reporting section and the current framework is starting to look difficult. It becomes more so for organisations that are operating globally. Google's global privacy counsel Peter Fleischer noted recently, in the context of a European Union (EU) investigation of Google's record-keeping practices, how "extraordinarily difficult it is for a global Internet company to function in line with different privacy standards in different countries".<sup>11</sup>

Businesses do find a way to work with this mix of laws and with the process obligations in the laws. However, the business response may not always help build trust. A compliance approach, where the law is not clear or it is inconsistent, can combine with an organisation's own decisions and behaviours and lead to trust breaking consequences including:

- staff fraud etc;
- management 'breaking or stretching the rules', for example CardSystems;<sup>12</sup>
- poor practice – data quality, use, disclosure, security; and
- considering security is a cost not investment.

In a similar vein, some organisations have taken a consent based approach to compliance with privacy principles. Privacy principles, for example the National Privacy Principles in the *Privacy Act 1988* (Cth), tie permitted uses and disclosures to the initial purpose of collection. However, possible uses may vary over time and while the first derivative may be very close to the original purpose, the sixth may not be very close. The tendency then is to write broad consents. While this may work into the short term it has to be seen against the sort of concern that individuals are reporting. In the words of the former Privacy Commissioner Malcolm Crompton in 2002 "Bundled consents are not good privacy or business practice and are totally contrary to the spirit of the Privacy Act".<sup>13</sup>

While there is some flexibility in general sets of principles, other laws are quite prescriptive and intentionally lock out other than permitted uses of personal information.<sup>14</sup> As discussed below, such laws are often an emergency regulatory response to an increased consumer reaction. While the short-term individual concern may be satisfied, the potential for future innovative use becomes much more problematic. Moreover, business models are usually built to work with the form of the current law. Radical or restrictive law changes are by their nature unpredictable and may be inconsistent with a business model requiring costly changes.

### 2.3. Information economy inputs at risk

---

<sup>9</sup> Office of the Privacy Commissioner Getting in on the Act: The Review of the Private Sector Provisions of the *Privacy Act 1988* March 2005 [www.privacy.gov.au/act/review/review2005.htm#provisions\\_work\\_balance](http://www.privacy.gov.au/act/review/review2005.htm#provisions_work_balance)

<sup>10</sup> Certainly, when looking at the privacy regulation in its broader context, the picture is less positive. The Privacy Commissioner's report, while taking the view that the provisions have worked well overall notes that provisions have failed to deliver a nationally consistent framework. Factors cited include disconnects between state and Commonwealth legislation and between the Privacy Act and laws in sectors including health and telecommunications. The report also points to regulatory responses to technological change as another source of inconsistency and uses the *SPAM Act 2003* as its example.

<sup>11</sup> See [www.bloomberg.com/apps/news?pid=20601085&sid=afa8mfVFOzdk&refer=europe](http://www.bloomberg.com/apps/news?pid=20601085&sid=afa8mfVFOzdk&refer=europe)

<sup>12</sup> See Federal Trade Commission media release of February 2006 which states that "CardSystems' failure to take appropriate security measures to protect the sensitive information of tens of millions of consumers was an unfair practice that violated federal law". [www.ftc.gov/opa/2006/02/cardsystems\\_r.shtml](http://www.ftc.gov/opa/2006/02/cardsystems_r.shtml)

<sup>13</sup> See [www.privacy.gov.au/news/media/02\\_8.html](http://www.privacy.gov.au/news/media/02_8.html)

<sup>14</sup> For example the credit reporting provisions in Part IIIA of the *Privacy Act 1988* (Cth) specify permitted uses and disclosure of credit reporting information by credit providers and credit reporting agencies.

The collation and analysis of huge amounts of information on many subjects and many people, in identified and statistical formats is an integral feature of the information economy. In the information economy, the highest valued use of data is often its use in a predictive context. The privacy issues here flow from the use of probabilities, which if applied without human intervention potentially lead to mistakes, discrimination in service, or other consequences for individuals. Done wrongly, it can also lead to a deep sense of 'Big Brother is watching'.

Mistakes can and do arise. The current telling example is probably that of individuals whose names end up on an airline watch list because they have an unfortunate name, or they fit a particular, probalistic, profile. Anecdotally, it is difficult or impossible to dispute a listing or get it fixed. The traveller may be pulled aside and if denied access to a flight bears all the inconvenience and cost, even if others such as airlines or government systems are totally to blame.

A key feature of the information economy is that it, and personal information, is networked. The World Wide Web provides consumer to consumer, business to consumer and business to business communication channels and networks. Businesses also transfer and share bulk data for a range of purposes and see potential value in extending this; for example to build better risk models or to analyse customer responses. Increasingly, new computing technologies and channels such as XML are facilitating business processes that involve instantaneous streaming and linking of data from many networked sources.

Privacy laws do not currently map well onto these business models. Privacy laws tend to assume binary relationships between individuals and organisations, not the networking of information and extended value chains that characterise both the World Wide Web and current business models.

If we are going to use personal information in innovative ways, there is the question of who bears the risk when things go wrong. Examples such as the one above contribute to people's sense of being out of control, the sense that things are going wrong and need to be fixed.

Some of the consequences of this angst are mentioned elsewhere in this paper. Here, the point is the impact on the availability of data sets to feed into the probalistics process. There is a trend here particularly in relation to the public data sets derived from various government activities, including land sales, motor vehicle registration, and the electoral system but also in relation to other public sector activities. As processing capacity and innovative uses increase there is a related tendency to respond to individual concerns by limiting access to specific authorised circumstances. In Australia, this has been the case for credit reporting databases, the electoral roll and the integrated public number database.<sup>15</sup>

## 2.4. Regulator frustration

Advocating for privacy law and finding a balance between privacy and other interest goes with the territory for a regulator. The task can become more frustrating when the law will not do the job that the community clearly wants it to; or when the law provides ineffective mechanisms to enhance consumer trust. The example of bundled consent mentioned above is a case in point. Interestingly, concerns of this sort appear to be common across jurisdictions. Equally it can be frustrating for regulators when they cannot respond flexibly to business needs in managing data.

Regulators agree that that an effective privacy solution goes beyond simply implementing privacy principles. The final communiqué from the 2006 Data Protection Commissioners' conference, which had as its focus the surveillance society, noted that:

- surveillance activities can be well-intentioned and bring benefits;

---

<sup>15</sup> The Integrated Public Number Database is an industry-wide database that contains information related to all listed and unlisted public telephone numbers in Australia, regardless of the service provider, for more information see [www.dcita.gov.au/communications\\_and\\_technology/policy\\_and\\_legislation/numbering/integrated\\_public\\_number\\_database\(ipnd\)](http://www.dcita.gov.au/communications_and_technology/policy_and_legislation/numbering/integrated_public_number_database(ipnd))

- unseen, uncontrolled or excessive surveillance activities also pose risks that go much further than just affecting privacy;
- privacy and data protection regulation is an important safeguard but not the sole answer;
- public trust and confidence is paramount.<sup>16</sup>

Privacy regulation has now been in place in a number of jurisdictions for a number of years and is a maturing branch of regulation. A reflection of this is the number of recent privacy law reviews: for example in Australia, Canada, and the United Kingdom. A theme of note in the submissions of Privacy Commissioners to the various reviews and inquiries has been the call for additional enforcement powers, and in the case of the United Kingdom, for penalties for certain privacy breaches. It is a timely warning that the current framework may not be delivering the level of privacy that communities are seeking.

### 3. How did we get here

This is a complex question and there are many ways of capturing the ideas. The points below are not meant to be the complete picture; rather they are a few thoughts to start the discussion.

#### 3.1. Information stores now and 40 years ago

The opening proposition for this paper was that designing a new approach to privacy and trust for the information economy was a high stakes enterprise. One way to illustrate this point is to observe the huge and growing amount of information, including personal information that is now being created.

The digital equivalent of 12 stacks of books stretching from the Earth to the Sun was created by humanity in 2006, according to new research:

In 2006, 161 exabytes (161 billion gigabytes) of digital information was created and copied, continuing an unprecedented period of information growth. This digital universe equals approximately three million times the information in all the books ever written. According to IDC, the amount of information created and copied in 2010 will surge more than sixfold to 988 exabytes, representing a compound annual growth rate of 57 per cent. The last time research of this type was attempted was in 2003 by researchers at the University of California, Berkeley, who came up with an information total of around five exabytes.<sup>17</sup>

#### 3.2. The 'Rules of the Game' as they are today

Most laws aimed at the protection of personal information are based on regulating various stages of an 'information life cycle'. The conventions that form the basis of data protection law have been designed to deal with discrete collections of data and discrete histories. They were based on the concept of transparency and individual control (albeit with increasing numbers of exceptions). Thus they usually provide that an organisation should:

- give notice to the person about whom it is collecting personal information, or even obtain consent to do so ;
- only collect the minimum information necessary to carry out its functions or provide the service involved;

---

<sup>16</sup> Information Commissioner's Office, United Kingdom Press Release 3 November 2006 available at <http://ico.crl.uk.com/files/Press%20release.pdf>

<sup>17</sup> "Humans created 161 exabytes of data in 2006", iTnews.com.au, 7 Mar 2007, ([www.itnews.com.au/print.aspx?CIID=74870&SIID=35](http://www.itnews.com.au/print.aspx?CIID=74870&SIID=35))

- identify the primary purpose of collection and limit its uses and disclosures of the personal information to that primary purpose or related purposes;
- keep the information secure, complete, accurate and up to date, sometimes being required to subject itself to compliance audits;
- allow individuals to see all the information held about them and obtain correction of errors and sometimes be able to require deletion of unwanted information; and
- de-identify or destroy personal information no longer in use.

The quintessential framework was promulgated by the OECD 1980; one of the most recent is the APEC privacy framework, adopted in November 2004.<sup>18</sup>

Privacy is also protected, of course, by a myriad of other laws, including anti-spam law, broader consumer protection law, telecommunications and postal legislation, administrative law such as Freedom of Information and Ombudsmen etc.

### 3.3. Burden of Notice and Consent

A notable feature of the principles above is the emphasis on process, in particular on notice and consent. The OECD Guidelines describe the intention of privacy principles as follows.

Generally speaking, statutes to protect privacy and individual liberties in relation to personal data attempt to cover the successive stages of the cycle beginning with the initial collection of data and ending with erasure or similar measures, and to ensure to the greatest possible extent individual awareness, participation and control.<sup>19</sup>

However, while experience is showing for example that requirements to give notice leads to lots of notices, it is not clear that they lead to more power or choice for individuals.

In fact, there is evidence that individuals can be overwhelmed but not enlightened by long disclosure statements, even where intended to allow informed consent. At the same time, the notice/consent process can be costly and time-consuming for business. Moreover, the current processes do not appear to encourage business to consider or mitigate privacy and information security risks for individuals. Consents and notice provisions may also be ill suited as the single control point in an information economy where data is networked and flowing rapidly, either over the World Wide Web or via bulk XML channels. These provisions do not allow business to deal easily with proposed novel uses of data.

Similarly, there is a view particular amongst business that access provisions impose cost and administrative burdens for little result particularly where an extensive search to reveal every mention of an individual reveals only fairly meaningless transaction data.<sup>20</sup>

There is an emerging view that excessive reliance has been placed on 'front end' mechanisms for individual control such as notice and consent to protect individual. This approach is based on the excellent but now ageing thinking from the 1960s by privacy pioneer, Alan Westin and does not take into account the realities of the way high volumes of personal information are collected used and disclosed in the current and rapidly evolving IT environment let alone the continued aggregation and

---

<sup>18</sup> "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", adopted by OECD member countries on 23 September 1980, online at: [www.oecd.org/document/18/0,2340,en\\_2649\\_34255\\_1815186\\_119820\\_1\\_1\\_1,00.html](http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_119820_1_1_1,00.html), and "Ministers Approve APEC Privacy Framework to Strengthen E-commerce and the Protection of Personal Information", Media Release from Asia-Pacific Economic Cooperation, 16 November 2005 with links to the Framework itself, online at [www.apec.org/apec/news\\_media/2005\\_media\\_releases/161105\\_kor\\_minsapproveapecprivacyframework.html](http://www.apec.org/apec/news_media/2005_media_releases/161105_kor_minsapproveapecprivacyframework.html)

<sup>19</sup> Organisation for Economic Cooperation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Explanatory Memorandum, paragraph 5 available at [www.privacy.gov.au/links/index.html#10](http://www.privacy.gov.au/links/index.html#10)

<sup>20</sup> *Access and Correction* paper presented by Jennifer Barrett, Global Privacy Officer Acxiom Corporation to International Symposium on Personal Information Protection Law, Institute of Law, Chinese Academy of Social Science June 2007

sharing by third parties<sup>21</sup>. It leaves individuals users bearing the risk in circumstances where they are not equipped, and as research is showing, not willing, to bear it.

The privacy principles we now work with were a function of the time in which they were developed. Then Professor Zelman Cowan in 1969 thought that what was needed was

not a Luddite smashing; it is a proper surveillance over the character and quality and relevance of the information stored by computer<sup>22</sup>

The first privacy thinkers were well intentioned. With the hindsight of forty years, it is possible to see them as working from a defensive design brief where computing and data processing were seen as a threat to privacy, a negative.

Against the reality of the massive increase in computing power it is perhaps time to move to more enabling framework, whether based on trust, stronger restitution or other measures.

### 3.4. Disconnect between business view and individual view

Whether privacy is conceived of as part of the claim to personal autonomy or in some other way, it is recognised as both a value and an emotional need for individuals.<sup>23</sup> The proposition here is that there is a disconnect between these sorts of concepts and a business view of privacy as a set of legal or compliance obligations.

While, as suggested earlier, any new approach is likely to continue to have principles or process rules at its base, the challenge will be to find a way to engage with individuals and satisfy their conditions for positive participation.

### 3.5. Development of the law in fits and starts

As noted earlier, the privacy landscape is made particularly difficult for business because of the unpredictable development of the law. The law tends to develop in fits and starts, with governments responding to, amongst other things, particular “hot button” issues or by making “emergency” response to shock events. In Australia, it is possible to consider that this approach has given us:

- Part IIIA of the *Privacy Act 1988* in response to developments in the credit reporting sector in relation to positive credit reporting;
- the *SPAM Act 2003* in response to the community concern about the huge increase in unsolicited email traffic; and
- the *Do Not Call Register Act 2006* in response to the continuing community resistance to telemarketing call to their homes.

Bob Gellman, an American privacy expert, notes a similar trend in the United State. In a recent presentation he noted there more than twenty laws with a bearing on privacy including:

- Fair Credit Reporting Act;
- Privacy Act of 1974;
- Gramm-Leach-Bliley (banking);
- Health Insurance Portability and Accountability Act (HIPAA);

---

<sup>21</sup> See “The Failure of Fair Information Practice Principles” by Professor Fred Cate in *Consumer Protection in the Age of the Information Economy*, Amazon reference [www.amazon.com/Consumer-Protection-Information-Economy-Markets/dp/0754647099](http://www.amazon.com/Consumer-Protection-Information-Economy-Markets/dp/0754647099)

<sup>22</sup> ‘A man without privacy is a man without dignity; the fear that Big Brother is watching and listening threatens the freedom of the individual no less than the prison bars’ Professor Zelman Cowan *The Private Man* The Boyer Lectures 1969 page 62

<sup>23</sup> Zelman Cowen, 1969, ‘The Private Man’, The Boyer Lectures, Australian Broadcasting Commission, p9-10

- Family Educational Rights and Privacy Act;
- Driver's Privacy Protection Act; and
- Children's Online Privacy Protection Act.<sup>24</sup>

The United States law continues to develop in this way, most recently in relation security breach notifications. In February 2005, in the context of a major security breach by the information broker ChoicePoint, privacy experts were reported as saying "the incident may convince other states to adopt legislation similar to the guidelines required by California".<sup>25</sup>

This prediction was borne out and by July 2005 in response to high profile security breaches "19 states have enacted notification laws and bills are pending in seven".<sup>26</sup> Today, over 38 States of the US have such laws.

In Australia, part of the intention in extending the *Privacy Act 1988* (Cth) to the private sector was to head off additional law. It is possible then to consider the development of the additional law as indication of failure of the Privacy Act. Whether this is the case is clearly a matter for debate. Part of the challenge for this discussion is to find an approach that delivers stable, predictable law.

#### 4. Economic value of doing better

At this point it is not possible to point to economic modelling that would say that in the right conditions of individual trust the economy would perform x points better. This paper suggests there is an arguable case, and that the economic benefits could be very strong. The thoughts below suggest areas that would be worthy of further consideration.

Information and communications technologies have driven economic growth and productivity at an accelerating pace over the past two decades. The first impact was in manufacturing with computer aided design and just-in-time inventory control. As we have moved further into the information age information and information technologies have become more associated with information that pertains to people. The former Chairman of the U.S. Federal Reserve Alan Greenspan told the U.S. Congress the best explanation for the delta between economic growth in the U.S. and Europe during the 1990's was U.S. industry's greater willingness to use new information technologies and information in business processes. In private conversations Greenspan supposedly said that the biggest payoff came from reducing knowledge float - the ability to predict with better accuracy future behaviour based on current knowledge.

The first big application of probalistics to data sets about people was in credit scoring in the United States. The U.S. credit bureaus began offering bankruptcy models in the 1980s that not only predicted bankruptcy, but also the risk of delinquency. Studies financed by the World Bank showed that the use of credit risk scores allowed lenders to provide credit to more individuals and at better prices. One of these studies, by Michael Staten and John M. Barron compared the Australian and United States modes and asserted that there would be economic benefits to collecting positive credit experiences in Australia.<sup>27</sup> There is some scepticism about both the research methodology used and whether it has correctly assessed the Australian context. However it provides some useful food for thought.

---

<sup>24</sup> Robert Gellman, Privacy and Information Policy Consultant, Washington, DC, [bob@bobgellman.com](mailto:bob@bobgellman.com), presentation to UNSW Cyberspace Law and Policy Centre Seminar, June 7, 2007

<sup>25</sup> [http://news.com.com/ChoicePoint+data+theft+widens+to+145,000+people/2100-1029\\_3-5582144.html](http://news.com.com/ChoicePoint+data+theft+widens+to+145,000+people/2100-1029_3-5582144.html)

<sup>26</sup> [www.namic.org/insbriefs/050707SecurityBreach.pdf](http://www.namic.org/insbriefs/050707SecurityBreach.pdf)

<sup>27</sup> John M. Barron and Michael E. Staten, "The Value of Comprehensive Credit Reports: Lessons from the U.S. Experience," in Margaret Miller, ed., *Credit Reporting Systems and the International Economy*, MIT Press (2003).

But the key point is that probalistics are rapidly expanding to other areas of the economy – including fraud and identity, health, business metrics as well as the more traditional marketing analytics.

Turning to another area, it is instructive to consider the explosive new business models that are growing up in the information economy. There are huge sums of money at stake; for example:

- News Corporation paid \$US580 million for MySpace;<sup>28</sup>
- eBay Inc. paid \$2.6 billion to purchase Internet phone service Skype International;<sup>29</sup> and
- Amazon’s worth is now \$15 billion<sup>30</sup>

In each case, these organisations are building a business where none existed before and these valuations are therefore only a fraction of the total economic value they have created when the value to other stakeholders in their businesses, including their customers, is taken into account. As noted above, recent comments by Google’s CEO underline the importance of an appropriate privacy and trust framework in maintaining these information based business models. There are also some telling examples of the economic loss from failure to protect privacy – a better approach to privacy, which puts the obligations on the body that is in a position to pay, may avoid more of these meltdowns:

- ChoicePoint “took a \$6 million charge in June after ID thieves duped the company into releasing personal data, exposing the information of as many as 162,000 Americans. The Alpharetta, Ga.-based data firm spent nearly \$2 million contacting affected customers and offering them credit reports and monitoring services. ChoicePoint also saw its stock price fall after the breach and now faces a possible class action lawsuit”;<sup>31</sup>
- Data Breach Will Cost TJX \$1.7B, Security Firm Estimates;<sup>32</sup>

It is fair to say that to date there have been no known privacy breaches of anything like these magnitudes in Australia. Of course this does not guarantee the future.

Finally, it is worth noting that economies such as India’s and many in Eastern Europe have used information and communication technologies to leapfrog ahead. India’s competitive advantage is not just cheap labour, but also skills in business process re-engineering. India has not been heavily impacted by privacy law; however that is beginning to change. A critical issue has been a lack of trust in the safety of information in India. So India is revising IT security laws, encouraging self regulation with teeth, and considering privacy law.

## 5. Stakeholders – what do they need

This paper is inviting seminar participants to consider a new approach to trust and privacy. If the intention is to move from heavily process based systems to something better, one of the challenges will be to decide if any new model can deliver a better outcome. One way to think about this will be to identify the interests of the various stakeholders and to test the model against these. The likely stakeholder groups and some initial thoughts about possible interests are set out below.

---

<sup>28</sup> <http://australianit.news.com.au/story/0,24897,20119094-15318,00.html>

<sup>29</sup> [www.businessweek.com/the\\_thread/techbeat/archives/2005/09/why\\_ebay\\_is\\_buy.html](http://www.businessweek.com/the_thread/techbeat/archives/2005/09/why_ebay_is_buy.html)

<sup>30</sup> Paul Festa, CNET News.com Published on ZDNet News: July 15, 2005, 4:00 AM PT [http://news.zdnet.com/2100-9588\\_22-5788988-2.html?tag=st.num](http://news.zdnet.com/2100-9588_22-5788988-2.html?tag=st.num)

<sup>31</sup> [http://searchsecurity.techtarget.com/originalContent/0,289142,sid14\\_gci1147324,00.html](http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1147324,00.html)

<sup>32</sup> [http://blog.wired.com/27bstroke6/2007/03/data\\_breach\\_wil.html](http://blog.wired.com/27bstroke6/2007/03/data_breach_wil.html)

## 5.1. Individuals

One possible set of thoughts, suggested by Marty Abrams in a recent presentation to some of the stakeholders, and based on a range of research, is that individuals will be confident and trusting where they:

- receive value and respect an information age;
- feel under control;
- feel secure;
- find use of personal information is based on expectations;
- are never surprised;
- get quick, effective resolution of their issues.

A recent collaborative research project between BT Group Chief Technology Office Research and Venturing and HP Labs set out to find what would be needed to encourage individuals to engage fully with ICT mediated services. While trust was an important element, the researchers concluded that the following were some of the key elements that needed to be addressed:

- restitution measures that are honest and clearly stated, and are guaranteed;
- control – increased transparency brings increased confidence;
- openness and honesty, for example about levels of security and protection, benefits and issues.<sup>33</sup>

Other factors that, based on experience, may need to be considered include:

- opportunities for anonymity;
- ownership in personal information and how value in use is distributed;
- the risk arising from any transaction and who bears this risk; and
- protection from disadvantage and discrimination flowing from the use of probabilistic or automated decision;

## 5.2. Business

As a starting point, and based on the discussion above, business interests in a privacy regulatory framework are likely to include:

- predictability of the regulatory process;
- freedom to innovate; , including the ability to use historical data in new, networked contexts
- flexibility;
- cost management;
- level playing field; and
- the ability to protect competitive advantages.

---

<sup>33</sup> Hazel Lacohee, Crane, S and Phippen, A, H *Trustguide: Final Report*, October 2006  
[www.trustguide.org.uk/Trustguide%20-%20Final%20Report.pdf](http://www.trustguide.org.uk/Trustguide%20-%20Final%20Report.pdf)

### 5.3. Government

Governments will only turn their attention to large scale privacy reform rarely. It is important that when they do, the reforms are farsighted and can respond flexibly to future emerging hotspots, so that further specific legislation is avoided, and government's own priorities can be accommodated.

In considering large scale privacy reform, the government's overall interest in any new approach will be to ensure it delivers on matters such as ability to facilitate economic growth, and competitive advantage and the impact that it may have such key priorities as community safety and satisfaction and border security.

Getting regulation of the information economy right means getting privacy regulation right. There are big benefits in enhancing consumer trust, and allowing business to create and unlock value. However, trust is more likely to be achieved, and Governments are more likely to regulate where there is wide stakeholder agreement on the core direction of change.

### 5.4. Regulator

The regulator charged with implementing a regulatory framework may be looking for some of the following features in the law itself:

- fits with individual concepts of privacy and does not need to be bent to fit;
- flexible and durable, works with the market to allow balances to be struck, avoid need for frequent new law;
- works regardless of the technology or the medium and is adaptable to organisational contexts (including size and business activity);
- provides for effective restitution and enforcement;
- includes the right obligations and incentives to promote compliance without depending too much on a macro central body;
- provides the regulator with the power or discretion necessary to ensure it can meet the expectations which business, consumers and governments reasonably have of it.

## 6. Foretelling and challenge for future

The final part of the paper looks briefly at some ways to go forward.

A first thought, in the context of the discussion above for example about individual's interest in honest advice about risks and swift and effective restitution, is to look at where the obligations in the system lie both for preventing problems and for fixing the problem when things go wrong. In this regard it is worth noting one commentator's view on security.

The current system does not provide incentives for organisations to actively improve the way they protect customer's asset security works best when the entity that is in the best position to mitigate the risk is responsible for that risk. And economics has a lot to teach computer security. We generally think of computer security as a problem of technology, but often systems fail because of misplaced economic incentives. The people who could protect a system are not the ones who suffer the costs of failure<sup>34</sup>

---

<sup>34</sup> Schneier on Security "Economics and Information Security", 29 June 2006, [www.schneier.com/blog/archives/2006/06/economics\\_and\\_i\\_1.html](http://www.schneier.com/blog/archives/2006/06/economics_and_i_1.html)

In economic terms this is the concept of internalising the externalities. It may be useful to look to other regulatory frameworks, for example the *Environmental Protection Act 1990* that aims to make the polluter pay for the cost of cleaning up a problem, for options to fine tune the risk allocation in the privacy regulatory sphere.

Another key question to consider is whether there could be a different check point in the system rather than over reliance on notice and consent. It may be possible for example to call for stronger governance, assurance and accountability arrangements, to support a range of options to provide notice. These requirements may vary according to the nature of personal information collected and the intended or likely future use. Again, it may be possible to look to other regulatory frameworks such as now applying in the financial sector. A feature there that may make a stronger assurance regime feasible is that the system pays for its own assurance – through requirements for external auditing and continuous disclosure and clear civil and criminal penalties.

In some circumstances human agents of some sort may be the answer; a person or organisation that could for example, keep track of and manage all the consents we have given. The human agent approach has been attempted. A well known example is the system of Caldicott Guardians established by the UK National Health Service. Caldicott Guardians “are senior staff in the NHS and social services appointed to protect patient information”.<sup>35</sup> Questions to consider here would be if, in the commercial world, it is possible to ensure that such an agent is genuinely acting in an individual’s interests and if such an approach could be economically viable.

## 7. Conclusion

The paper’s proposition is that a privacy regulatory framework that promotes trust and confidence for individuals and facilitates business efficiency and innovation is a key enabler for the full enjoyment of the benefits of the information economy.

The privacy regulatory framework is of course only part of the solution. Other elements include improved public understanding of the issues, better technologies, appropriate identity management and stronger governance structures. However, the regulatory framework plays a critical role and if working well will compliment these other elements.

The enterprise is one of potential great value and interest to community both as a way to unlock economic value and to make the society one we want to live in.

---

<sup>35</sup> “NHS Caldicott Guardians”, available on the UK National Health Service at: [www.dh.gov.uk/PolicyAndGuidance/InformationPolicy/PatientConfidentialityAndCaldicottGuardians/AccessHealthRecordsArticle/fs/en?CONTENT\\_ID=4100563&chk=ZdxTGp](http://www.dh.gov.uk/PolicyAndGuidance/InformationPolicy/PatientConfidentialityAndCaldicottGuardians/AccessHealthRecordsArticle/fs/en?CONTENT_ID=4100563&chk=ZdxTGp)