

World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

Volume 8, Number 7

July 2008

Commentary

Legislation and Guidance

Global internal investigations: How to gather data and documents without violating privacy laws.	3
Belgium: Enforcement action on the rise.	5
Free parking in Ostend.	6
Data Security Council of India: A self-regulatory organisation.	6
United Kingdom: Employers steal the march on dishonest employees.	11

Personal Data

Safe to play, a trust framework for The Connected Republic	15
Italy: New rules on personal biometric data in the banking sector.	25

News

Legislation and Guidance

Australia: Privacy Commissioner releases case notes for 2008	12
Europe: Recent findings from the Article 29 Working Party's plenary session.	12
United Kingdom: ICO takes action against double-glazing cold calls under PEC Regulations; Information Commissioner appoints RAND Europe to assess European Data Protection Law; Government may opt out of European Union PNR agreement	13
United States: Organisations adopt guidelines for electronic personal health records	14

Personal Data

Asia Pacific: The 29th Asia Pacific Privacy Authorities Forum	26
Canada: Privacy Commissioner funds research and public awareness projects	26
Europe: EDPS adopts opinion on programme to protect children online	27
Europe/United States: Deal on data sharing near; E.U. citizen sues U.S. over data sharing.	27
Hong Kong: Further data losses at HSBC	28
Ireland: Irish Commissioner critical of United States court ruling	28

Italy: Launch of Italian Institute for Privacy	28
New Zealand: Privacy Commissioner issues recommendations for updating privacy law	28
Sweden: Public outcry over eavesdropping law	28
Switzerland: Swiss Privacy Commissioner releases his annual report	29
United Kingdom: Virgin Media loses bank details of 3,000 new customers; Daily Mail publisher loses data on thousands of staff, suppliers and contributors; Information Commissioner's Office is to issue enforcement action against the HMRC and MOD; Marks & Spencer to appeal ICO's enforcement action; Privacy International unhappy about launch of Google's Street View	29
United States: Judge orders Google to hand over YouTube user data	31



www.bnai.com

Personal Data

International

Safe to play, a trust framework for The Connected Republic

*This is an edited version of a white paper written by the Global Public Sector Practice, Internet Business Solutions Group and Cisco, for which Malcolm Crompton and Robin McKenzie from Information Integrity Solutions were the lead consultants.**

Malcolm Crompton and Robin McKenzie can be contacted at: MCrompton@iispartners.com and RMckenzie@iispartners.com

Introduction: the trust dilemma in a connected world

Connectedness is emerging as the defining characteristic of our time. The ability to share information and ideas quickly, cheaply and increasingly pervasively is having a profound impact on our sense of ourselves, our instinct for community and voluntary exchange and our capacity to innovate products, services and experiences.

It's not that being connected is anything new in itself or that the ability to communicate and share hasn't always been close to the heart of the human experience. But there is something about the intensity and reach of the more densely networked lives we are creating that suggests something more than simply an evolution.

Nowhere do these profound and unsettling changes have as much impact as they do in government and the public sector. Confronting the consequent possibilities and risks for public policy and the design and delivery of public services is, in many different ways, taxing governments around the world.

Cisco's overall response to this challenge is framed by a piece of thinking we recently updated as "The Connected Republic 2.0" or TCR:2, which explores the potential of technology not just to improve public service delivery but to change the very business of governing.

We think that active and engaged citizens are at the heart of the transformation of the public sector. The new tools of communication and collaboration enabled and accelerated by the network, especially the social network which we describe as the collaborative web (often called Web 2.0), empower citizens and bring them together in new ways.

The technology combines with, and to a large extent is driving, a way of thinking about how individuals engage with governments that is not only going to produce better, more responsive public services, but also stronger communities.

We are witnessing technology-enabled change linking to larger concerns of public sector reform and democratic renewal. In this new environment, eGovernment is becoming more central to what government itself is becoming –

orchestrating the creation of public value by putting people and communities at the centre of responsive networks of knowledge, service, trust, and accountability.

We think there are three characteristics that underpin this changed environment. They will have a major impact on the way governments operate and the way policy makers must think. In this new world:

- The network becomes an essential platform for collaboration and creativity;
- Public value is created as governments "empower the edge" to make the best use of all available expertise and experience;
- Harnessing the "power of us" becomes part of a new public policy business model to create knowledge, solve problems and deliver better services.

This is a model of public management that builds on, but moves beyond the limits of the "new public management". It is a model that relies on, and feeds, an ethic of high trust and openness. It assumes that knowledge, expertise, and insight are dispersed throughout communities and at all levels of formal and informal power. It assumes that there are new types of social knowledge and information, forged and refined in the interactions between citizens, communities and governments that will make a difference to the complex social and economic problems we are trying to solve. From this perspective, one of the central tasks of governing – over and above the enduring obligations of law and regulation, taxation and redistribution, and security – is to find ways to connect that dispersed knowledge and wisdom in ways that make a practical difference to the way policies are developed and programs are designed and delivered.

The collaborative web is changing forever the way governments work and behave. But while it brings astonishing possibilities, for many its potential is clouded by uncertainty about the significant risks with which it comes pre-loaded. The many practical questions about whether and how governments should engage with its possibilities have coalesced into a persistent and potentially debilitating doubt how can we be sure that it is "safe to play" in this connected world?

The answer is actually quite simple – only if the invitation to engage is on terms that are worthy of being trusted. But what does "worthy of trust" really mean? This question has been the subject of much debate among commentators on the information economy. The primary task of this paper is to cut through this debate and provide a distinctive frame within which to think about trust and how it grows, or can be destroyed, in the collaborative web environment.

In seeking to create trust you need to look at three areas: control, fair risk allocation and accountability. What makes them powerful is the way they interact. What we're suggesting is that the way these three elements work together in a constantly changing pattern of mutual influence and support will play a significant part in determining how safe people feel in a more open, connected world.

Addressing these factors requires a combination of both new and old strategies: maximizing the use of the exciting new tools, the collaborative web itself underpinned by old fashioned, good public administration on the other.

The focus of this paper

Continuing concerns about trust and security offer persistent obstacles to the more rapid and comprehensive take up of online service delivery and citizen engagement in the 'connected republic' model of governing, which is based on much wider use of the Internet and new network-enabled tools for communication and collaboration.

This paper offers some ideas about how that fundamental challenge of trust can be more effectively dealt with as governments embrace the vision, principles and solutions of the 'connected republic'. For the most part, the paper concentrates on those interactions between government and citizens that involve the delivery of services and, to a lesser extent the exchange of ideas and opinions as part of a wider democratic conversation.

While the focus of the paper remains on the relationship between citizens and government within a new model of governing, it inevitably touches on larger questions about how people and communities respond to the new demands and possibilities of a more connected world. Part of the uncertainty with which the paper is concerned is about whether governments themselves should embrace the connected world of Web 2.0. Another part of the uncertainty is about citizens wondering if they, their information and their privacy will be safe as they increasingly interact with businesses, with governments and with each other in a more connected world.

We believe that these two concerns – how citizens deal with government and how people live in a more connected world – are two dimensions of the same question. Not only is it hard to separate those issues out, but in many ways they are interdependent. We think the way the paper reframes the trust issues more generally offer insights into both dimensions. But the principal purpose of the paper remains to stimulate thinking about how to improve the trust dimension of the citizen-government relationship.

Finally, a word of caution. This paper is not intended to be a comprehensive or definitive compendium on trust in government. Its main focus is on some aspects of trust in the online world. On the other hand we believe that this paper's insights into trust and how it is gained may also have some relevance for gaining trust in the offline world.

Understanding the risks of the collaborative web

The easiest way to capture the essence of the connected world is to think of the rise of social networking,¹ including MySpace, YouTube, Facebook, LinkedIn, as well as blogs,² and wikis.³ Platforms or applications providing these kinds of

features are sometimes called "Web 2.0" We will call it the collaborative web.

Platforms and applications of this kind are often interactive and encourage, indeed rely on, users themselves to develop their own content. They enable users to share information and to fashion and benefit from a collective intelligence whose essence is collaboration and co-creation. In other words, instead of insight, intelligence and authority coming from 'the top' or 'the centre', they are increasingly produced by the same people who consume them. Many of the new Web 2.0 applications make it easier to collect and share intelligence on users' interests and behaviours and to create value from this information.

Government in a collaborative web environment makes use of all the new platforms to facilitate improved service provision and more responsive government, to enable people to establish conversations with government and to arrange government services in a way that suits them rather than on a take it or leave it basis.

Government is not only a direct service provider, of course. It also discharges important roles including providing for national security, law enforcement and regulation about which individuals have little (legal) choice even if they might have consequences that are adverse to their individual interests. Our focus in this paper is primarily on those areas where services are provided to citizens over which those citizens have some discretion. It does not pursue in any detail the different challenges of a trust model for services such as law and enforcement and national security.

However, we must recognise that citizens' awareness of the imperatives of these and other government activities may have an impact on their willingness to trust government in relation to its direct service provision activities.

What risks are we talking about?

There are many risks that contribute to, or can undermine, trust in the connected world. They include those relating to transaction fulfilment, for example. But this paper focuses on the risks that we believe are critical to the way people thrive in the collaborative web environment, both in their interaction with government and more widely in their interactions with business and with each other, because the collaborative web relies so heavily on information about people for its energy. In this paper when we refer to risk we are principally focusing on the risks associated with information aspects of security, identity management and privacy.

*Security*⁴

In the rush to exploit the new capabilities of the collaborative web, security issues have often taken a back seat with the result that the risks and vulnerabilities are only gradually becoming understood.

We are discovering that the collaborative web opens up whole new opportunities for those interested in making mischief or engaging in criminal activity on the Internet. Interactive features being added to websites and web services using new programming techniques provide a much greater "attack surface" than before. As one commentator⁵ has put it,

"a traditional Web site is like a house with no windows and just a front door. An AJAX Web site is like a house with a ton of windows and a sliding door. You can put the biggest

locks on your front and back doors, but I can still get in through a window.”

Also, at the human level, social networking sites expose information to many more people than those to whom it would be exposed in most offline personal relationships and that information can easily be reused and redistributed by third parties.⁶

As awareness of these vulnerabilities rises, citizens may be increasingly concerned about engaging with government initiated web services, particularly where they are required to provide sensitive personal information.

Identity management

Identity management, or the need to ensure that where necessary only known and authorised individuals gain access to networks and systems and the resources contained in them has also emerged as a major risk.

Up to this point much of the collaborative web has developed without much thought about whether identity management is needed and, if so, what kind. We have tended to assume that people using the technologies can be trusted to do the right thing.

However, safely managing identities, real and virtual, may be more central to the success of the collaborative web in the government environment than we might have allowed. For example, recent incidents in which a disgruntled ex boyfriend placed false and demeaning information on his ex girlfriend's page, and another where a fake and defamatory MySpace webpage demeaned the reputation of a politician,⁷ are examples of the risks users of these sites increasingly face.

But, somewhat ironically, there is just as much a risk of over reacting which could lead to the mistake made by many in the Web 1.0 environment which was to over-compensate by insisting on identifying people wanting to transact on the Internet even when the offline equivalent did not require it. Governments have fallen into a similar trap by developing “Rolls Royce” identity management solutions covering all government transactions which have then been rejected as too expensive and too intrusive for many of the everyday low security interactions people or businesses might have with government.

Besides the obvious risks to personal privacy, over reliance on authenticating identity assertions also creates new security risks. The unintended consequence of over reliance on identity as the key to trust essentially is simply to increase the value proposition behind stealing identities or creating false identities.

*Privacy*⁸

The essence of information privacy risk is that an organisation might deliberately use, or allow other people to see or use, information in ways people neither want nor expect.

A person's identity is what links together all the information flowing around the Internet about that person. The trust dilemma here is that linking personal information can be both beneficial and harmful. It can create value for individuals and organisations operating in the collaborative web. On the other hand, the risk can be unwanted contact, discrimination, embarrassment or even physical harm. It may also cause people to change their behaviour in ways that have undesirable consequences for wider social outcomes. They

may avoid using the web or provide false information even when it really matters. The outcome of such uses may or may not be well intentioned.

We can see the dilemma in more concrete terms if we look at social networking sites. While these sites enable people to make connections in exciting and beneficial new ways, they also massively facilitate connections that people don't want or expect.

Examples of unexpected uses include employers who scan social networking sites as part of an employment process and university officials who search for photos of students to determine who may have taken part in end of term high spirited partying.⁹

Facebook is also facing the stark reality of the consequences of unexpected uses in the protest about its News Feeds and Mini-Feeds aimed at keeping every member abreast of every change in the lives of linked up “friends”.¹⁰ More recently, the same problem emerged in an initiative by all 50 State Attorneys General in the United States to accuse the social networking site of not keeping young users safe from sexual predators and failing to respond to user complaints.

Individuals and service providers are only just coming to terms with the complex ways that people expect to be able to conduct their social lives and the difficulty of trying to reflect, nurture and enable the subtleties of social relationships in the off line world. A more subterranean issue yet to emerge for users is an understanding of how information about their interests and behaviours is used by social networking platform providers, such as search engines, for purposes unrelated to the facilitation of social networks. We are all learning the consequences in the connected world of the reminder that “there is no such thing as a free lunch”.

Citizens weighing up how to respond to the spreading influence of the collaborative web as a platform for their interactions with government are likely to bring to bear this kind of learning when they decide how they should respond. Those having experienced the rocky road of exposing information about themselves in social networking contexts are unlikely to embrace the new government services with the same naïve enthusiasm of the early days of MySpace and Facebook. Add to this mix persistent and pervasive fears of “big brother” resulting from increasing government surveillance in response to terrorism and law enforcement imperatives we can see that governments seeking to embrace the potential of the collaborative web may face significant obstacles.

How government adapts to the “collaborative web”

Governments have to come to terms with the risks associated with providing services in a collaborative web environment if they want to reassure citizens that it is “safe to play”. But where to begin?

Up to now, the focus has mainly been on addressing weak security and identity management, using technology as the main solution, and then *only from the point of view of the needs of the organisation*. As the paper explains later on, this is a fatal weakness that has to be redressed in any successful trust regime.

This focus has widened to a more user centric approach with the help of analysis by Crompton (2004)¹¹ the response by the

London School of Economics (LSE) to the U.K. Identity Card proposals¹² and Microsoft's Kim Cameron's set of "Laws of Identity" which much more clearly align with the dynamics of the collaborative web's hyper-connectedness.¹³

However, new thinking is needed to help us tackle the trust dilemma. We have to start with risk and the way it interacts with control and accountability as the elements of a framework that will cut through the uncertainty to offer a more robust platform for policy and practice.

The significance of risk allocation

There is a critical issue that governments are missing when they implement new projects in the connected web environment. That issue is risk – how it is allocated and how it impacts on citizens. Drawing on the work of Malcolm Crompton at Information Integrity Solutions, this new way of thinking goes to the heart of citizen concerns.

The relevance of risk allocation has increased as organisations focus much more on their own risk management. This focus is emerging more into wider public consciousness, particularly as too often, risk management *has not resulted in reduction of aggregate risk but rather reallocated the risk from the organisation to its employees, clients or service users.*¹⁴

In particular, consumers are sensing that organisations too often manage their risks by expecting their consumers to bear an increasing and inappropriate burden of the risks associated with consuming their services. They are also waking up to the fact that service providers seek to hide this shift in risk by changing the channel through which a user receives a service, for example, when closing face to face services and opening call centres or other forms of remote contact including online. Risks include being left to manage technical failures or privacy and financial losses through online security breaches.

For example, shifting customers onto an online service in order to reduce costs often shifts a number of risks to the customer. These include security risks, unreliability risks, and the costs of acquiring the necessary technology in order to be able to engage with the service or, if the costs are prohibitive, the risk of spending increased time in queues in order to receive a face to face service.

Some of these risks have been obvious to individuals while others have only emerged where organisations have been forced to tell people about them, for example, through data breach laws. This trend towards shifting of risk to individuals and away from organisations is a major factor in undermining trust in the connected world.

Our analysis is supported by research funded by the U.K. Department of Trade and Industry which resulted in the publication of the "Trustguide" report.¹⁵ The report breaks new ground with considerable potential to advance the search for a robust and pragmatic platform to lift trust and confidence in the connected world.

The research took a "citizen centric" approach to understanding the beliefs and needs of users in relation to trust, security and privacy in ICT mediated activities. From facilitated focus group discussions, one cross cutting theme emerged in the research:

"While an initial hypothesis may be that people do not engage with online services because they do not trust them, our findings have shown that trust is not as significant a

measure as first thought. *What is more important to understand is that people are willing to take risks online, as long as they are informed, and it is clear how consequences will be addressed.* People use specific services not because they trust them, but because they in some way provide a benefit to the individual and they know that if something goes wrong, restitution will be made."¹⁶ [Emphasis added]

The Trustguide research places great emphasis on education and information because it enables better informed risk decision-making. Individuals engage with services if they can make an informed decision about whether it is worth the risk to engage. It considers a more educated online society is more likely to be willing to use services provided in novel ways because knowledge brings confidence and control. The Trustguide research indicates that people are rightfully sceptical about technology, but if empowered and allowed to experiment, they tend to adopt solutions that are socially beneficial. It advocates giving individuals the chance to learn through doing.

A dynamic system linking risk allocation, control and accountability

The role of risk in establishing trust is better understood if we look at how it interacts with two other concepts, control and accountability. When people say they don't trust an organisation, it is likely that these are the three things they are actually worrying about even if they might not articulate their concerns in these terms.

Risk and its allocation

Service users become uneasy and feel that this is a game in which it is not "safe to play" – if they don't know enough about the risks of using a service and how the service has defined and allocated the risks they do know about.

This unease is reinforced if users get a sense that they are being asked to shoulder increasing levels of risk such as when the channel for service provision changes.

Control

Risks they are concerned about include that they will lose control over what happens to information about them or that they have insufficient control over how that information is demanded, collected and stored in the first place. This sense of loss of control is heightened if they do not understand enough about the entity to which they give personal information or other entities that may have control over the information.

Accountability

Finally, and underpinning other user concerns, is the concern that too often organisations, with which people interact and which collect and use information about them, fail to demonstrate full accountability for the way they manage risk or to accept responsibility quickly and effectively when risks manifest themselves as failures or breaches. While organisations manage their failures with business continuity plans, the equivalent is often strangely 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.

These three factors are significant because of their interaction. In that sense, they are interdependent: if you only deal with issues in one or even two of the elements, it's likely you will fail to impact the trust dimension. Sometimes they are complementary; at other times they are not. A common reaction to a perceived increase in personal risk, for example, is to demand increased personal control. Another example is the way greater accountability can be used to reduce risk significantly. Each component must be addressed to achieve rising levels of trust.

If we want to lift trust, which is central to lifting the take-up of online services and citizen engagement with governments more broadly on the collaborative web, then policy and practice has to keep all three of these elements in the right balance.



Towards a sustainable trust framework for government: lessons from the private sector

But what happens to the trust system we have outlined here when a government embraces the ethic and potential of the collaborative web? Is it applicable to public sector service provision? What impact will it have on other aspects of public administration and governance?

On the question of trust in government initiated services, there is considerable evidence to suggest that citizens are just as concerned about government services provided using new technologies as they are when services are provided by private sector organisations. Indeed there is reason to suspect that citizen concerns could be even greater where governments are providing services for at least three reasons:

- the lack of regular contact citizens may have with some government services – which make it more difficult for citizens to learn to trust a service through direct experience;
- the lack of choice citizens may have in relation to some government provided services, for example paying taxes, updating electoral roll data, or receiving essential health, housing or welfare services, which may diminish the power of citizen control as a trust mechanism;

- the unique power government has in society, including the ability to pass laws that provide for data sharing between its other agencies or other governments, with reasons ranging from law enforcement and national security to service delivery improvement or policy analysis which may generate “big brother” fears in citizens.

It may be that the trust issues applying in the public sector environment are different only as a matter of degree compared with those of private sector organisations rather than fundamentally different. We think experience in the wider collaborative web context can provide insight into making it “safe to play” for the citizens receiving egovernment services.

Reframing the trust dilemmas confronting governments as the interaction between basic concerns about control, risk and accountability prompts some fundamental questions. The answers should guide policy and practice in the design and delivery of services in the collaborative web environment.

Some of those questions include:

- How should the risks associated with engaging in government services in the collaborative web environment be defined, allocated and managed?
- What special approaches to risk and its allocation might be necessary in a context where citizens have only limited or no opportunity to make choices about, or exercise control over, the services they receive or the manner in which they receive them?
- How do we ensure that governments seeking to implement the kinds of models envisaged in the Connected Republic are able to manage newly emerging risks as the collaborative web evolves?

Our answer to these questions builds on a foundation that combines pragmatism with a strong and confident embrace of the central features of the connectedness that itself is creating many of these complex trust dilemmas in the first place.

Firstly, we accept that the connectedness we are witnessing and experiencing is an undeniable, unavoidable and irresistible phenomenon with which we must come to terms. At the same time, it is full of potential for social and economic development and a sense of engagement and empowerment. It gives governments and citizens the chance to share knowledge and gain the benefits of thinking together.

This collective “intelligence” in both senses of the word can fuel innovation and speed up the innovation cycle to solve problems and create opportunities. It has great potential to enhance democratic processes.

Secondly, we start from the premise that the undeniable risks inherent in providing government services in a collaborative web environment are manageable. Allowing an irrational and extreme response to the very real concerns on which those risks are based is itself a risk.

We should not assume that the dangers for privacy, security and identity management are terminal. Rather, the trick is to make these trust dilemmas a friend and not an enemy. Building robust policy and operational frameworks that assume the need for high standards of trust and accountability will not only diminish risks and lead to better policy and program outcomes but fuel the further spread of the connected world and its opportunities.

Thirdly, we think that one of the keys to meeting the trust challenges posed by the control, risk allocation and accountability framework lies in our ability to harness the instincts, values and the capabilities of the connected world to provide the solutions we need.

The very features of the connected world that can create risk can also provide the platform and tools from which solutions will evolve. The network's effect as a platform for connection, communication and collaboration will be as essential to managing the risks of the collaborative web as it is to enabling, and often accelerating, the very connectedness that gives rise to those risks in the first place. Paradoxically, the network is as much a part of the solution as it is a part of the problem. The network, combined with a renewed focus on doing the basics of public administration well, becomes a central part of the solution.

So the argument is that:

- the move to a more connected world is inevitable and, we believe, overwhelmingly a good thing;
- even though its inherent risks are daunting, they are manageable; and
- the best way to address those risks is to build the capabilities of the connected world into the heart of the way we design and implement our response.

While these insights frame the trust dilemma in the 'connected republic' in a way that we think will prompt better policy and practice, we also have to accept that there is no magic bullet answer to the questions we have posed. We know that what we set out here is not going to solve all the trust problems that governments will encounter as they come to terms with providing services in a collaborative web environment. We also know that a range of approaches and tools will be needed. The approaches we outline here may need to be backed up by law, or facilitated using technology.

Using collaborative web capabilities to solve collaborative web problems

Turning back the tide is not the answer to the trust dilemma. Governments will miss a major opportunity for renewal, better services and policy improvements if they do not capitalize on the values, instincts and capabilities of the collaborative web to help solve many of the trust dilemma problems. Looking at examples such as the development of OpenID there is no doubt that this is already happening in the private sector at an incredible pace, and that there are lessons for government in how to do it.

OpenID is an approach to identity for the Web 2.0 world (and beyond) which is rapidly gaining credibility and take up. It is a decentralised, user-centric URL (or URI) based identity protocol. The URL based approach allows us to decentralise the brokering of our identity and to keep our identity information in the place we choose. It does away with the need for Internet users to have multiple user names and passwords and to enter information about themselves every time they register on a new website.

The decentralisation exists on a number of levels:

- Users can host their identity on any server they choose, without having to ask anybody for permission or

approval; they can also choose to have it hosted by one of the growing number of OpenID hosting services.

- Service providers can choose from a variety of software implementations offered by a variety of vendors and Open Source projects.
- The OpenID specifications are developed in an unencumbered, meritocratic process that is open to participation by anyone who shows up.
- Anyone can use their own technical innovations within the OpenID framework, even if they replicate, or compete with the OpenID specifications themselves.¹⁷

These are attributes that speak directly to the values and ethic of the collaborative web. They make it easier for users "at the edge" to make decisions about managing their identity and to harness the power of the network to integrate the OpenID capabilities with specific tools and technologies that users themselves add. Control, unequivocally, rests with people who use and rely on the system and not with the system itself. It is a solution that is gaining considerable support.¹⁸ And it is a solution whose impact is entirely a function of the quality and reach of the connections enabled by the network that links people, information and services.

While providing for user-centric control and facilitating decentralisation of holding of personal information looks like a good start, there remain security issues and the need for stronger identity authentication in some circumstances. But what is different about OpenID is that it seems to provide a good platform to enable people to solve those other "real" problems as well.

It also appears to transform the way personal information is managed and transmitted within separate and discrete social network spaces and, in doing so, might solve some of the issues of user control over personal information we have identified in this paper.

An example is WikiScanner, a response to a concern about a lack of transparency associated with alterations to Wikipedia. Rather than require upfront identity authentication from those who change content, it searches the change logs to identify the organisation associated with the IP addresses recorded with changes and then uses the network to make them public. Part of the impact is that it creates a kind of "name and shame" effect on behaviour. But it also enables people to assess the accuracy of the content they are reading. Much as the basic Wikipedia model itself, the solution relies on the collective intelligence and transparency of a community of users able to quickly and easily share information and insights across a robust network. It is another example of the attributes of the collaborative web providing the foundation for a solution to many of the difficulties to which they give rise.

Reputation-based feedback mechanisms such as those used by eBay also have considerable potential to address a number of the trust issues faced on the collaborative web world without over working the need to rely on authentication of identity assertions. Not without significant potential risks of its own, this reliance on the community of users to "share and care" enough to be able to form its own "police" function creates a force for openness that offers a powerful antidote against the loss of privacy and security.

So what is the significance of these examples? The most basic observation they reinforce is that, in order to function

safely and effectively in a collaborative web environment, you have to think and act like the collaborative web. If governments fail to engage with the attributes and instincts of hyper-connectivity, they will find it harder to counter its real threats and may, by relying only on old tools and attitudes, risk making the problems worse.

The sooner governments start to understand this new world and come to grips with both its potential and its risks, the sooner they will start to craft the right mix of policy, regulation and operational behaviour more likely to increase one without fuelling the other. Failure to start, and then to sustain, that journey risks leaving government badly trailing in the field of effective trust models for service provision in the collaborative web environment.

Good public administration

Governments cannot ignore growing citizen concerns about trust in public services offered in and on the collaborative web. But we know that the factors affecting citizen trust in government are not new. They have a very long history. In many cases, the pillars of public administration that underpin democracy have evolved over a long period precisely to deal with these concerns.

We need to understand therefore that the dynamic system for generating trust we have outlined will not dispense with the need for governments to also ensure that the more traditional components of public administration and governance continue to be applied to this new way of providing government services. To maintain a solid foundation on which to build citizen trust, governments must continue to ask, and answer well, such questions as:

- How are decisions made?
- Who is involved and consulted in decision making?
- Who needs to be informed of the decision?

First, how are decisions taken? The capacity exists with these technologies to think about more transparent and robust processes for decisions at all levels of an organisation. The ability to empower the front-line staff through information to deliver personalised and joined-up services can devolve decision making within a public accountability framework, leaving senior management to deal with strategic matters and policy deployment. The challenge however is to maintain consistency and accountability and appropriate feedback mechanisms in this new decision making environment.

Without appropriate mechanisms, the citizen could be left bearing the brunt of “buck passing” when things go wrong with people higher up the line unwilling to adhere to decisions made lower down if it does not suit them, or admit that there are structural rather than one-off problems.

Second, who is involved and consulted in decision making? The ability to consult online and engage with a wider community in ways that was previously impossible can be powerful in legitimising outcomes. A recent private sector example illustrates the consequences of not listening in the face of these new capabilities. The HSBC bank changed its overdraft offer to recent graduates. Within days, a backlash occurred through a community emerging on Facebook, calling on students to boycott or leave HSBC. The bank was forced to reverse the decision through the power of the network. Of

course, the challenge to the public sector is to overcome the problem of “listening only to the loudest”.

Third, who needs to be informed of the decision? Many of the hardest challenges in the public sector require speedy and accurate interaction across internal boundaries and also with other organisations outside government.

An obvious example is the protection of children at risk, requiring co-ordination between education, health, social care, justice and police, charities and others. The power of the network as a platform for enhancing these complex interactions has significant potential to mitigate the information gaps and poorly informed judgments behind the tragedies that have occurred in the past with these difficult cases. The risk here is that lazy solutions are adopted that drag more people into the net of information sharing than need to be. At worst, it could mean that everyone is treated as if they are a potential abuser of children when, in reality, the potential perpetrators are a much smaller percentage.

Strategic recommendations for government online services

We have emphasised the importance of risk and its impact on citizens. We have also explained its interdependence with control and accountability. We can now explain how to use these concepts to achieve trust when providing government services, combining collaborative web tools with practices essential to good public administration.

Fair risk allocation

Providers of public services are failing to recognise that if they want to be trusted, they cannot just manage their own risks. They must also consider the significant additional risks that their users face.

Strategies could include:

- When commissioning a risk assessment for a new service, make sure that it also includes service user risks;
- When implementing continuity plans based on that risk assessment, make sure that they provide for continuity for service users as well as the service provider;
- Paying particular attention to citizen risk where individuals have limited direct control in relation to a service; for example, where you expect presentation of identities backed by high integrity enrolment, you should also address user risk and offer equally strong mutual authentication of your service both as a sign of respect and as an additional security measure for users;
- Building in a User Impact Assessment process as a standard step when developing a new service. This can help to identify citizen risks that are often overlooked and provide a framework to consider how to mitigate or allocate those risks;
- Start with a strong presumption that the service provider should bear the risk particularly where citizens have little or no control over whether, or in what manner, they receive a service or where the government, for whatever reason is not in position to be as transparent as it might be.

Control

A key to managing control in the collaborative web environment is to take a user-centric approach to service delivery. Services as much as possible should make it easy for the citizen to choose how information about them is collected, used and disclosed. But to make it effective and easy, we have to move away from the old fashioned approaches to control which rely on up front information and bundled consents provided in a context where people cannot understand or absorb the information, do not understand the implications and cannot conveniently make a real choice. Government will have to be more imaginative in gradually helping citizens to understand how to exercise the kind of control they seek.

Strategies could include:

- Moving away from providing a “one stop shop” service through one government portal, and instead enabling citizens to build their own platforms through mashups and other collaborative web tools. This gives citizens that capacity to solve emerging trust and risk issues for themselves, and minimize the amount of information collected about users;
- Setting initial defaults for information handling to a “privacy respecting” option, for example, setting the default at not sharing information across government agencies and empowering the user to specifically opt in if they wish to share information in this way;
- Making it easier for users to change these settings once they understand the benefits and risks of new ways of connecting or interacting with government services. It is good manners to assume that people will want as much practical anonymity and as little unnecessary interactions as possible. No one wants to be bombarded with messages that aren’t relevant to their situation;
- Providing citizens with the chance to experiment in a safe environment so they learn through doing and gradually exercise greater control as they understand and further grow to trust the new service;
- Presenting information and the “opportunity to consent” at the points in a process that are most relevant.

Transparency is another feature that facilitates control and trust. Citizens are more likely to trust governments the more transparent they are about the way they operate. This is true too for government agencies and individual government services. Citizens are able to make better choices if they are fully informed. There is evidence that citizens may be willing to exercise less direct control over their information where there is a strong culture of transparency. This is because they can be more confident that the government has the information under proper control, and that citizens will know if that is not the case. The strong history of Freedom of Information laws that apply in Scandinavian countries, for example, may be part of the reason why citizens in those countries have a more trusting attitude to the national identity card approach.

Governments must analyse what levels of control they can and cannot give to their citizens when they provide a service and assess the implications of that level of control. Where governments, for whatever reason, must reduce or eliminate citizen control over personal information, they must be aware of this potential weakness in the trust system and compensate

for it by giving greater emphasis to risk identification, allocation, and accountability in order to achieve the necessary levels of trust in service users.

As governments adapt to social networking techniques to provide services, they will need to avoid the pitfalls into which many social networking sites themselves have fallen. People expect to be able to manage their relationships in a way that closely mirrors the way they conduct them in the offline world. This means that services using social networking platforms and capabilities will need to ensure that people are able to have subtle and fine tuned control over the relationships involved in actually delivering the service. Citizens will feel they have greater control if they are able to start, develop and finish relationships in the same way that they do with real people in the real world. This philosophy also underpins approaches being taken in developing identity management technologies to fit with the collaborative web world (for example, the approach to identity management taken in Microsoft’s CardSpace initiative).

Accountability

Accountability has two main strands – good governance and an effective safety net.

Good governance is critical to ensure that an organisation spells out clearly what it will do in terms of allocation of risk and control, and very importantly, is able to prove it is doing what it said it would do. Governance mechanisms are best provided in a layered approach starting with internal management metrics and feedback backed up by top management. Governance mechanisms should also include external accountability, for example, to ministers, regulators and continuous disclosure obligations.

Strategies could include:

- Exploring ways to build the voice and values of customers into your governance mechanisms;
- Using feedback mechanisms similar to eBay’s auction and rating system in order to gain citizen feedback on government initiated web services. This helps to evaluate services and provide a strong incentive for services to lift their game in all respects including on privacy, security and trust more generally;
- Regard internal and external feedback as an opportunity to generate trust, and constantly improve a service, rather than a threat – do not try to control or censor feedback information;
- Make sure that front line staff can frankly and fearlessly contribute to the constant improvements. This means a clear feedback or comment moderation policy which might exclude offensive, actionable or irrelevant material, but should tolerate most other material, even if uncomfortable.

Using the new capabilities erodes the strict distinctions, and institutional divide, between those who design, manage and deliver public services and those who consume them. That doesn’t diminish the enduring responsibilities of government service agencies for the quality, ethics and impact of their own work. But it does suggest a richer mix of inputs to the difficult and often sensitive judgments that are the focus of many governance decisions.

Identity, privacy and security failures will happen regardless of the quality of the education, legal, technological or governance strategies in place. These can minimise the chance of failure but do not eliminate it. Also, some risks are still emerging and so cannot be managed in advance. As the Trustguide research shows, service users are increasingly aware that no service or system is foolproof or failure safe. Therefore knowing there are strong restitution and safety net procedures in place has a positive impact on the risk people perceive.

Strategies could include:

- Having internal complaints handling and trouble shooting that is welcoming, easy to use and available outside office hours if needed;
- Having appropriate external mechanisms as back up for handling complaints that cannot be settled internally;
- Starting from the position that the citizen has done the right thing and acted responsibly and in good faith, until there is clear evidence to the contrary;
- Making use of collaborative web platforms such as a wiki or blog to enable users who have experienced problems and solved them to help each other through information exchange. This could be through a government platform or by making external sites that do this easily referenced.

Regardless of the approach taken, mechanisms for making it “safe to play” when engaging in new services or new service channels will inevitably become out of date, for example, because of new technology, or because individual behaviour changes. Any framework must therefore build in means of identifying, understanding and responding to such change. This will help individuals feel that it remains “safe to play” because the support they receive responds in a systematic and well thought out way with no major time lags that may otherwise leave individuals bearing an unfair burden of risk once again.

Another key element, therefore, is a trust system that can learn, thriving in a culture of self-knowledge and adjustment that itself is enabled and accelerated by the use of networked tools of communication and collaboration.

Strategies could include:

- Nimble review and regulatory mechanisms where legislation establishes a basic compliance framework while the detail is left to expert standards setting, as occurs in many significant industries;
- Built in, more serious and periodic review mechanisms, for example, legal policy review bodies such as the Law Reform Commission in Australia;
- Rapid response to user feedback that identifies service improvement, security weaknesses or even incorporation of shared, user designed “spaces” within government established social networks;
- Work with the fast-developing ecosystem of external commercial and open-source solutions. Watch out for what works. Most proposals won’t, and you don’t want yours to be one of them.

Conclusions: key principles and checklist

At the heart of this approach to the trust dilemmas inherent in the collaborative web environment is the need for governments to start thinking differently about the policy and operational model to produce the kinds of trust outcomes they want.

Principles

The approach we have adopted in this paper can be distilled into the following principles, providing a practical guide for governments as they explore new ways to build high trust into all dimensions of service provision.

Fair risk allocation

- Focus on risk for all parties – including the citizen – identify, allocate and be clear and specific about ways to mitigate it. Align the incentives so risk is managed by those best able and motivated to manage it. In particular, look after citizens when they are ill-equipped to look after themselves.
- Regularly review risk settings to make sure they evolve appropriately in line with the dynamic nature of the collaborative web environment.

Control

- Don’t hide behind consent if the service user has no real choice.
- Be prepared to pay greater attention to mitigating citizen risks, accountability and a safety net where direct citizen control is not possible.
- Give citizens as many options as possible about how they manage their relationships in the online world; make it possible for them to conduct them as they would in the offline world if they wish to.
- Encourage a culture and practice of learning; realise the best solutions will emerge from user experience and small, regular and inevitable system adjustments; enable people to understand and discover the capabilities and risks of a new service gradually and in a safe environment; encourage adaptive solutions that utilise the “power of the edge”.

Accountability

- Be prepared to be more transparent.
- Have strong internal and external audit and review mechanisms to demonstrate trustworthiness.
- Ensure that there is a good safety net for citizens when service delivery fails them in some way. Credible restitution (for example, for identify theft) is worth more than over-promising a foolproof, perfect system.
- The network is part of the solution; use collaborative web strategies to solve collaborative web problems. Connectedness can solve, at least in some measure, the problems it creates.

Checklist

Here are some questions that policy makers and program designers could ask themselves:

- Do you agree allocating and managing risk, control and accountability are the key to achieving trust in service delivery in the collaborative web environment?
- How do you currently assess risks when you are establishing a new service? Do you include the risks to service users in your assessment?
- Who currently bears the risks associated with your service? Are they in the best position to bear it?
- Are your risk assessment mechanisms “future proof”?
- What would happen if a service delivery fails for service users? What plans do you have for dealing with service failure?
- To what extent, as you try to balance risks, are you prepared to draw upon the values and insights of your service users? Do you make that easy to do and simple to manage from their perspective?
- Is walking away from your service a realistic option for an unhappy service user? If not, what other mechanisms have you for gaining their trust?
- Have you thought about the tools the collaborative web gives you to enhance customer control, better manage risk and provide for greater accountability?
- Are you prepared to be honest and straightforward about the goals and purposes of the service you are providing and they way you manage customer information to achieve those purposes?
- Are you robust enough to receive, and publish without censorship or spin, the feedback you receive through collaborative web mechanisms such as blogs or wikis?
- In administering government services provided in a collaborative web environment, have you thought about, and engaged your users in discussing, these questions:
 - How are decisions taken?
 - Who is involved in decision making?
 - Who needs to be informed of the decision?

* An earlier draft of the paper was presented at the Public Services Summit hosted by the City of Stockholm and Cisco, Stockholm, Sweden, December 10, 2007.

A full version of the paper is available for download at www.theconnectedrepublic.org where it was first published. This is a community space, developed by Cisco’s Internet Business Solutions Group where people can meet, share their thinking and link up with each other about the world of connected government and politics, often termed Government 2.0.

- 1 A social network service focuses on building and verifying of online social networks for communities of people who share interests and activities, or who are interested in exploring the interests and activities of others, and which necessitates the use of software.
Most social network services are primarily web based and provide various ways for users to interact, such as chat, messaging, email, video, voice chat, file sharing, blogging, discussion groups, and so on. In general, social networking services, such as MySpace, Facebook and Bebo, allow users to create a profile for themselves. Users can upload a picture of themselves and can often be

- “friends” with other users. In most social networking services, both users must confirm that they are friends before they are linked.
- 2 A blog is a user-generated Website where entries are made in a journal format and displayed in reverse chronological order. Blogs often provide commentary or news on a particular subject, such as food, politics, or local news; some function as personal online diaries. A typical blog combines text, images, and links to other blogs, Web pages and other media related to its topic. The ability for readers to leave comments in an interactive format is an important part of most early blogs. (Source: <http://en.wikipedia.org/wiki/Blog>)
- 3 A wiki is a Website that allows visitors to add, remove, and otherwise edit and change content, typically without the need for registration. It also allows for linking among any number of pages. This ease of interaction and operation makes a wiki an effective tool for mass, collaborative authoring. (Source: <http://en.wikipedia.org/wiki/Wiki>) Perhaps the best known example is Wikipedia itself – an encyclopedia collectively produced by volunteer Web users who supplement and edit each other’s content.
- 4 When we worry about information security, we are concerned that an organisation or some other person to whom we have given information might not keep our information safe from unauthorised or inappropriate access (whether internal or external). We might also worry that somebody else might steal information directly from us via our computer.
- 5 See Billy Hoffman, quoted in Joris Evers, The Security Risk in Web 2.0 July 28, 2006 CNET News http://news.com.com/The+security+risk+in+Web+2.0/2100-1002_3-6099228.html?tag=st.prev
- 6 www.zdnet.com.au/news/software/print.htm?TYPE=story&AT=339281191-130061733t-110000002c
- 7 www.smh.com.au/articles/2007/08/09/1186530526713.html
- 8 Privacy has other aspects not covered in this paper, including bodily privacy and territorial privacy.
- 9 www.cbsnews.com./stories/2007/07/17/tech/main3067887.shtml
- 10 See eg “Facebook and the Politics of Privacy”, MotherJones.com, September 14, 2006 at www.motherjones.com/interview/2006/09/facebook.html.
- 11 See for example “Proof of ID required? Getting Identity Management Right”, Office of the Privacy Commissioner, www.privacy.gov.au/news/speeches/sp1_04p.pdf
- 12 See “The Identity Project, an assessment of the UK Identity Cards Bill and its implications” released in June 2005 and related papers at <http://is2.lse.ac.uk/idcard>
- 13 Kim Cameron developed these laws as revealed laws in the same sense as other natural laws such as Newtonian mechanics were seen as revealed laws of nature. Just as Newton’s laws were later seen as part of a wider framework, Cameron clearly countenances that the Laws of Identity may later be seen as part of a wider framework. He developed the Laws of Identity in a collaborative blogging process over the months leading to their finalisation in May 2005. The Laws are online from Microsoft websites and his own blog, www.identityblog.com/?page_id=354
- 14 See for example, SMH, Ross Gittins Opinion, Jan 31, 2007, (www.smh.com.au/news/ross-gittins/risky-business-but-not-for-the-boss/2007/01/30/1169919337040.html); Governor of the Reserve Bank of Australia, 2006 Boyer Lectures (www.abc.net.au/m/boyerlectures/stories/2006/1769905.htm) and internationally Jacob S Hacker, The Great Risk Shift, 2006 Oxford University Press.
- 15 Trustguide: Final Report, October 2006, Hazel Lacohee BT Group Chief Technology Office, Research & Venturing, Stephen Crane, HP Labs and Andy Phippen, University of Plymouth, Network Research Group, online at www.trustguide.org.uk.
- 16 Trustguide p 1
- 17 The Case for OpenID Phil Becker December 4, 2006, Digital ID World <http://blogs.zdnet.com/digitalID/?p+78>
- 18 “CardSpace/OpenID Collaboration Announcement”, Identityblog, February 6, 2007, www.identityblog.com/?p=668