Information Privacy and Trust in Government: a citizen-based perspective from New Zealand

Rowena Cullen
School of Information Management Victoria
University of Wellington

Patrick Reilly
Fulbright Fellow 2005
Victoria University of Wellington

Abstract

Increasing use of e-government has raised issues about the privacy of information provided by citizens to government. This paper explores the experiences and concerns of New Zealanders in relation to information privacy, and the impact of these concerns on the trust they place in government.

A series of focus groups were conducted among a range of community groups. The findings reflect a range of attitudes about information privacy and the trustworthiness of government, and centre around two major themes: the use of technology and concerns about the competency of and practices of government employees. Most respondents were unaware of their existing protections; preferred face to face communication; had low levels of confidence in the privacy of online communication but made use of it for convenience sake; had greater confidence in government than in commercial organizations but made distinctions between individual agencies. Breaches of privacy were shown to have a negative impact on trust in government.

1.Introduction

Throughout the world, information and communications technologies are changing the way governments operate and interact with citizens. These technologies have also changed the way individuals' information is collected, processed and stored, making it more readily available than ever before, and potentially liable to breaches of privacy. The purpose of this study was to investigate the relationship between privacy and trust, with an emphasis on how citizens' concerns about information privacy are related to the level of trust they have in government organizations. From a citizen's perspective, information privacy contributes to personal autonomy and dignity, and the right to privacy is one of the fundamental tenets of liberal democracy. At the same time, democratic governments depend on a contract of trust between citizens and the state. Building trust has become a key principle of New Zealand's e-government strategy [1].

This study therefore asked a number research questions:
1. What are New Zealanders' concerns about their information privacy?
- What influences these concerns?
- To what extent are people aware of the existing protections of their right to privacy?
- To what extent are people aware of the options for redress if they believe their privacy has been breached?
2. How trustworthy do New Zealanders believe government organizations are in relation to information privacy?
3. When an individual believes an organization has violated their privacy, does this impact on that individual's trust in that organization?
4. If one government organization breaches an individual's privacy, does this affect the individual's perception of the trustworthiness of other government organizations as well?
5. When individuals need to provide personal information to government organizations, in which channel do they have the most confidence that their privacy will be protected?
- What influences the level of confidence?
6.What are New Zealanders' attitudes towards using the Internet to communicate personal information?

2. Literature Review

This study is concerned primarily with information privacy, which involves "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others" [2]. The fact that privacy is acknowledged and valued across many political systems is evidenced by Article 17 of the *International Covenant on Civil and Political Rights*, which states: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation" [3]. Similar protections are also supported in Article 12 of the *Universal Declaration of Human Rights* [4].

While privacy is necessary to an individual's personal autonomy and dignity in a modern democratic state [5], at the same time privacy is not an absolute right. In certain situations, an individual's right to privacy may be outweighed by the public interest in the disclosure of personal information (e.g., the location of convicted sexual offenders' residences, or the salaries of certain government employees). Thus, it is argued,

trade-offs must be made to promote a balance between these seemingly competing interests [6]. This need for balance has led to longstanding debate about how to determine what is a "reasonable" trade-off. Etzioni argues that, in many instances today, individual privacy is over-valued relative to the public interest and common good, to the detriment of society [7], and Westin notes, "either too much or too little privacy can create imbalances which seriously jeopardize the individual's well-being" [8]. Regan also suggests that the value of privacy may not be limited to the individual, but may also have "common, public, and collective purposes" [9].

2.1 Trust, and 'trust in government'

The notion of trust has also been the focus of considerable academic debate [10], although there is some consensus around a few key points: trust is empowering (and therefore valuable) in many interactions, and while trust is most often developed over time, it can be lost quickly. Trust has been defined as "a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another" [11]. This is equally true of governments. As far back as feudal Chinese society during the fifth century BC, Confucius affirmed that trust is the most important resource for a government, "if the people have no faith in their rulers, there is no standing for the state" [12]. Contemporary research suggests that, in modern democracies, citizens' distrust of their government may have an adverse effect on the effectiveness of that government [13].

It is important to acknowledge that the concept of the citizen's trust in government is different from interpersonal trust. Trust in an individual is based on a judgement concerning the trustworthiness of that person, based on knowledge or some other perception Our ability to assess the trustworthiness of an organization is related to our expectations and knowledge of that organization including the intentions and competence of the individuals in that organization. Given that governments are comprised of thousands of individuals working in hundreds of organizations, a citizen's attempt to evaluate the trustworthiness of their government may be considered a formidable challenge. Indeed, Hardin argues that the notion of 'trust in government' is fallacious and implausible because "the knowledge demanded by any of these conceptions of trust is simply unavailable to ordinary citizens" [14]. Despite this claim, as Bennett and Raab observe "elevating the level of the public's 'trust and confidence' in business and government has become something of a *mantra* in this contemporary discourse and practice" [15]. However, while there have been a number of attempts to identify the factors that most significantly influence citizens' trust in government,

there remain significant gaps in our knowledge about how to effectively promote and maintain the public's trust in government.

U.S. studies indicate that Americans' level of trust in their government has decreased significantly since the early 1970s [16]. Research into New Zealanders' attitudes towards their government indicates a similar decline in trust, and also suggests that citizen's mistrust of government is not related to government performance [17]. This apparent decline in public trust has occurred despite New Zealand's consistently high rankings in Transparency International's *Corruption Perceptions Index* which ranks the country's government amongst the least corrupt in the world [18].

2.2 Government and citizen's personal information

In many situations, the provision of personal information to government organizations is compulsory. This contrasts with the nature of information exchanges that individuals engage in with private organizations, where individuals may make decisions about which organizations they provide their personal details to. Thus,

> governments have special privacy obligations arising from the concept of democracy, which includes the establishment of rules mediating the power relationship between government and citizens [19].

Governments collect personal information from citizens for many purposes, including taxation and social welfare benefits. The collection of information in these cases is justified by the requirement to determine liability or eligibility, and may require highly personal financial and health-related information to be exchanged [20]. The implicit sensitivity of this information highlights the importance of ensuring that the information is handled properly and used only for the purpose for which it is collected. Since individuals in lower socioeconomic groups are typically thought to be more reliant on government welfare programs, it is often suggested that these sections of the population are more susceptible to invasions of their privacy. However, Raab and Bennett suggest that, while lower classes may be more vulnerable to certain risks, different social classes are vulnerable to different privacy-related risks. Specifically, they note

> those who are further up on the socioeconomic ladder are more likely to be part of the credit-card economy and to be targeted with considerable precision by direct marketers and the private sector in general [21].

2.3 Privacy and trust online

Fukuyama, has emphasized the important role trust plays in interactions and relationships involving the

Internet [22], a view supported by the findings of Friedman, Kahn and Howe, who suggest that one primary difference related to trust in the online environment is the greater challenge individuals face in trying to "reasonably [assess] the potential harm and good will of others" [23]. As Solove observes, "the general progression from information collection to processing to dissemination is the data moving further and further away from the control of the individual" [24], which may be related to increases in the level of public concern about privacy. Thus individuals' privacy concerns may be related to perceptions that they do not have control over their personal information [25].

High levels of concern over personal information,, especially in the online environment, have emerged in a recent survey of the attitudes of a stratified random sample of New Zealanders aged 19+ conducted by telephone by Consumer Link for Unisys Asia Pacific in August 2006 [26]. This showed that 54% of respondents were 'very concerned' or 'extremely concerned' about unauthorized access to or misuse of their personal information (85% in total expressed some level of concern). Further exploration of this data shows that concern is affected by region, gender and other factors such as socioeconomic status (concern is greater among blue collar workers). Higher numbers of female respondents (57%) and higher numbers of Christchurch respondents (78%) were 'very' or 'extremely' concerned, compared with males (49%) and those living in Auckland (44%). The same methodology was employed in Australia in May 2006 [27]. While 56% of Australian respondents reported being 'very concerned' or 'extremely concerned,' Australian levels of concern over national security are higher than in New Zealand, 41% of Australians are 'very' or 'extremely' concerned over national security, compared with 29% of New Zealanders.

Other research specifically focused on gauging New Zealanders' views about interacting with government online suggests that, in comparison to other countries, New Zealanders have an above average perception of 'safety' in providing personal information to Government over the Internet, that this perception of safety has increased considerably among groups of New Zealanders who routinely use online government services. [28] This is reinforced by research showing that. while privacy and security issues are sources of concern to New Zealanders, and while some individuals believe they have little control over their personal information, and that government data sharing activities could potentially reduce their confidence in government, New Zealand citizens have greater confidence in government websites compared to websites in general [29].

2.4 E-government, privacy and trust

Privacy-related issues and concerns are a critical challenge for successful implementation of e-government. In the U.S., many Americans acknowledge the potential benefits of being able to interact with government online, yet significant numbers also have concerns about the privacy and security of their personal information submitted through government websites [30]. An investigation of the current state of, and challenges facing e-government in a number of countries suggests that "*all countries face the same challenges of balancing information privacy against potential service enhancements.*" The same report indicates that, although there are significant potential advantages of data sharing amongst government departments, "*refining legislation and policies to support information sharing without undermining privacy protection continues to be a critical obstacle to effective interdepartmental integration*" [31].

2.6 Challenges of investigating privacy

Given the complexity of the concept of privacy, any research investigating privacy issues must be carefully designed and implemented, in order to ensure that researchers and participants are using similar concepts of privacy. Many surveys have asked questions about "how concerned" individuals are about privacy, yet these simple questionnaires often fail to investigate the nature of these concerns or identify the associated causes [32].

Some research has suggested that an individual's privacy concerns are directly related to their perceived vulnerability, and perceived ability to exercise control over their own information [33], or that people do not understand the "real implications of privacy and security in the Internet age," and since they are oblivious to the issues, they are currently unable to address the problem [34]. Other research has indicated that online privacy concerns are related to the amount of experience an individual has using the Internet, concluding that as experience grows, privacy concerns are reduced [35]. Awareness of some of these issues has driven the research design used in this study.

3. Methodology

This paper presents findings of one part of a larger study that used three instruments for collecting information from different groups of New Zealanders. A series of eight focus groups were held in and around the Wellington region, with an average group size of seven individuals. In a separate but related study, a series of semi-structured interviews were conducted with individual representatives of specific groups of New Zealanders. Another section of the New Zealand population identified as having valuable information to

contribute to the research consists of those individuals who believe that their privacy has been breached. A survey questionnaire was designed and used to collect information from those individuals who had submitted privacy-related complaints to the Office of the Privacy Commissioner (OPC). These associated projects are not reported here, but can be found in the full report of the project [36].

The focus group interviews gathered both quantitative and qualitative data about individuals' beliefs, attitudes and feelings on information privacy, and gave participants an opportunity to explain their views. Each participant completed an initial questionnaire consisting of general questions about concerns about their personal information and their trust in the government. Where appropriate, in an effort to avoid uncertainty inherent in phrases such as "how much do you trust 'Organization X' to protect your privacy?" the questionnaire used phrases like "how confident are you that 'Organization X' will handle your personal information properly and adequately protect it?" By 'operationalizing' the concepts of trust and privacy in this way, the research sought to minimize the possibility of participants giving generalized answers to the questions. The group interview followed, including a discussion of five general questions and five scenarios for discussion, which were designed to present individuals with a situation involving an improper flow of personal information to get as realistic a view as possible of their responses to breaches of privacy. The groups comprised: two groups of parents (of school-aged children) in different social contexts, university students, recent immigrants, members of city branch of a business association (industry leaders and CEOs of large corporations), small business operators, Maori (the indigenous people of New Zealand), Pacific people (both immigrant, and New Zealand born). Each focus group meeting was recorded and transcribed and the data was coded, using a hierarchical framework of themes. The coding schema is available in the report of the full project.

4. Findings

Tables 1 and 2 present basic demographic information about the focus group participants.

Table 1. Focus group participants - Gender

Gender	Number	Percentage
Female	33	56.9
Male	25	43.1

Table 2. Focus group participants' age

Age	Number	Percentage
15-19	2	3.4
20-29	14	24.1
30-39	15	25.8
40-49	9	15.5
50-59	6	10.3
60-69	8	13.7
70+	4	6.9

The questionnaire was used to collect information about participants' activities online, specifically whether they use online banking, Trade Me® (online auction website)[1] and/or make purchases from online stores. This data is presented in Table 3.

Table 3. Participants use of online services

Online Activity	Number (n = 58)	Percentage (%)
Use online banking	29	50.0
Use Trade Me®	21	36.2
Purchase from online stores	15	25.9

Half of all participants reported that they use online banking, a figure comparable with research suggesting that 41% of New Zealanders had used online banking as of October 2003 [37]. Although more current figures would be helpful, it may be reasonable to presume that this percentage has increased somewhat in the past two years, which would seem to indicate this group's use of online banking is approximately consistent with national statistics.

4.1 Concerns, Attitudes and Behaviors (prior to discussion)

The initial questionnaire also asked participants to indicate their level of agreement to a series of statements about their privacy-related concerns, attitudes and behaviors (using a Likert scale from 1 = Strongly Agree to 5 = Strongly Disagree.). Responses to these questions are shown in Table 4.

Many of the issues referred to in these statements were also addressed in the group discussions. For example, responses to statements S7 and S8 enable a comparison of whether participants have more

---

[1] See www.trademe.co.nz

confidence that their privacy will be protected by government organizations or private businesses, and this question was also raised later in discussion, when participants were asked to explain their responses. Response data for S6 suggests that a significant majority of participants are concerned about the privacy of their personal information when it is communicated via the Internet. Responses to S7 and S8 indicate only a slight gap between participants' levels of confidence in government organizations and private organizations. In contrast, the gap between the percentages of individuals who agreed with S11 compared with S12 seems to imply that individuals are more likely to look for the privacy policies (or other statements about how their information will be used and handled) on web sites of private businesses before providing their personal information.

Statements receiving a high percentage of neutral responses, e.g. S10 and S13, may imply that participants did not know enough about the topics involved. For instance, the fact that nearly a third of participants responded "Neutral" to S10 may suggest that many individuals were unsure about how much information the government holds about them (this was also supported by comments made in group discussions).

The final question in the survey (Q16) asked each participant about their level of trust in government organizations, and the majority of participants (58.9 percent) reported that they trust all government organizations the same amount. However, in the subsequent discussion, individuals' comments seemed to contradict this view, as most said that they trust some departments more than others.

Table 4.   Reported attitudes, concerns and behaviors

Statement (n = 58)	SA[*]	A	N	D	SD	% Agree	Av[**]
S6. I am concerned about the privacy of my personal information when it is exchanged online via the Internet.	31	19	5	1	0	89.29	1.57
S7. I feel confident that my personal information will be handled properly and be adequately protected by the *private businesses* (e.g., stores, banks, etc.) I deal with.	11	22	14	8	2	57.89	2.44
S8. I feel confident that my personal information will be handled properly and adequately protected by the *government organizations* I deal with.	13	22	13	7	2	61.40	2.35
S9. I trust government employees to treat my personal information with appropriate respect for my privacy.	15	19	11	11	1	59.65	2.37
S10. I am generally concerned about the amount of information that various *government organizations* hold about me.	15	15	16	6	4	53.57	2.45
S11. I usually seek or check statements about the way in which my personal information will be protected before I supply information to *government organization*s.	18	19	11	7	2	64.91	2.23
S12. I usually seek or check statements about the way in which my personal information will be protected before I supply information to a *business* that I deal with.	20	25	8	5	0	77.59	1.97
S13. I think the rules governing the way in which government organizations collect and exchange information about me are adequate.	3	25	19	7	3	49.12	2.68
S14. I sometimes refuse to provide information to a government organization if I feel they do not have an adequate reason to ask for such information.	11	30	8	5	4	70.69	2.33

* Abbreviations: SA = "Strongly Agree"   A = "Agree"   N = "Neutral"   D = "Disagree"
               SD = "Strongly Disagree"   Total Agree = (Strongly Agree + Agree)
** Av = Average Response (1 – 5, where 1 represents Strongly Agree and 5 representsStrongly Disagree)
The lower the mean score, the more strongly participants tended to agree with the statement.

A significant proportion of respondents (41%, n=23) made distinctions between government agencies in terms of trust, although the majority (59%, n=33) did not do so. Asked which government organizations they trust the most, as well as those they trust the least, participants named Inland Revenue Department as both the least trusted (equal with the welfare agency, Work and Income NZ) and as the most trusted organization (followed by the Ministry of Health). Other responses to this question included: "not sure," "I just don't trust any of them," and "they are all the same."

4.2 Data from discussions

The eight focus group interviews provided more in-depth data from the various perspectives of the participants involved. Since the course of each group discussion was influenced by the comments made by its participants, a number of issues were discussed in some groups and not others. Participants' gave various definitions of the concept of privacy. Many indicated that they believed privacy is related to being able to control "who knows what" about things related with their private lives. Some defined privacy in terms of types of information that they feel should be kept private and confidential (e.g., related to health, finances, etc.). Other individuals, predominately in the group of Pacific peoples, explained that their view of privacy is primarily concerned with keeping family information private and protecting the honor of their family's name and reputation.

One of the first questions posed to groups was about whether individuals were aware of any laws or regulations that exist to help protect their privacy. Most commonly, there was uncertainty amongst the group about any such protections. However, once someone had mentioned the Privacy Act others would acknowledge that they had heard of it although the majority of individuals reported that they knew little (if anything) about that Act.[2] On the other hand, in some groups there was at least one participant who was familiar with Privacy Act because of their occupation. In these cases, the individual with this familiarity explained how the Act applied to their job, and shared what they knew about the provisions of the Act. Despite those with a basic understanding of some provisions of the Privacy Act, the overwhelming majority of participants reported knowing little or nothing about what protections (laws, regulations, etc.) or which organizations, e.g. the Office of the Privacy Commissioner (OPC), or the Human Rights

Commission, etc., exist to help protect their right to privacy.

Participants expressed various views about their willingness to complain about situations where they believed their privacy had been breached. While some claimed that they would seek redress, many participants affirmed that they were unlikely to complain about minor breaches of their privacy. Individual comments suggested that some believed the existing complaints processes (via the specific organization and the OPC) were likely to take too long, were unlikely to be effective, and would not be able to remedy their dissatisfaction (i.e., contending that after privacy-related harm is done, most often any resulting damage cannot be undone or rectified).

Participants were asked whether they have more confidence that their personal information will be handled properly and adequately protected by government organizations or organizations that are not part of the government. Overall, the majority of individuals reported having more confidence in government organizations.[3] One response that was consistent with the attitudes of many participants was:

> *I think a private organization is more likely to* sell my information*, whereas government would be more likely to* lose my information.

Many comments suggested that individuals believe the objectives and motivations of government organizations are more virtuous (and therefore, more trustworthy) than private sector entities. On the other hand, some participants voiced concerns about data sharing between and amongst government bodies, an issue discussed further below

When individuals were asked to explain why they had more confidence either way, different views were evident:

> *I think* government*. I would feel better with [government] than a private organization personally because I feel that [*government organizations *are] audited all the time and they're quite accountable…*

in contrast to:

> *I would be more inclined to trust* private *organizations, …* Government *seems to, more and more, want to pry into personal activities.*

Individual's responses seemed to be influenced by their occupation. Some people working in the private sector were adamant about how serious their organizations were about protecting their customers' privacy, while others who work for (or with close relatives working for) government expressed similar

---

[2] Regardless of whether participants were aware of the Privacy Act, many individuals responded to the question by saying that their privacy is supposed to be protected based on which "boxes they tick" on the various forms they fill out.

[3] Although we did not ask specifically about the banking sector, individuals in most groups noted that they felt banks were the most trustworthy organizations with regard to privacy.

views supporting government organizations. Participants were also asked whether they considered some government organizations to be more trustworthy than others or they trust them all the same. The vast majority reported that they assess the trustworthiness of each organization separately, and therefore, they trust some more than others. In these discussions, very few people said that they trust all (or even most) government entities equally. Those who trusted all government organizations similarly were more likely to report low levels of trust.

Participants were asked to name the departments that they trust the most and the least, and explain why. In particular, individuals were encouraged to try to articulate what influenced their assessment of an organization's trustworthiness. Some individuals reported that they believe organizations whose objectives are not directly linked to money are more trustworthy than those that are, citing this as a cause for distrusting IRD and Work and Income (WINZ), among others. Similarly, a number of comments implied that some organizations have developed more reliable or trustworthy systems for collecting and processing personal information.

Individuals provided explanations about why they trust some organizations more than others and these were almost always based on their familiarity with, and personal knowledge of, each organization. Most specified that the amount of influence any source of information (about an organization) would have on their attitude is directly related to the credibility of the source. Generally, knowledge gained through personal experiences was reported to have the most influence, followed by stories or information received from friends and family, and lastly, information received through different media channels (television, radio, newspaper, etc.) Participants reported that there were many government organizations that they knew little about (those that they had no experience with, and were unlikely to interact with in the future), and therefore, could only generalize about the trustworthiness of those organizations. In cases where individuals expressed a high level of confidence in a particular organization, they commonly attributed this confidence to their personal experiences with that organization.

When participants were asked whether a breach of privacy in one government organization would affect the amount of trust they have in other government organizations, the overwhelming majority reported that only their level of trust in the specific organization would be decreased. A few individuals indicated that it might affect their assessment of the trustworthiness of government organizations in general based on their experiences with one or two specific organizations.

4.3 Confidence in various channels

Participants were asked which channel they considered more trustworthy for providing personal information to government. The overwhelming majority of respondents reported the most confidence when they provide their personal information in a face-to-face environment (this was consistent across all groups). The next most preferred channel for providing personal information was the post. However, this question generated a lot of diverse answers. In many groups, the Internet was slightly preferred to the telephone, but not compared to face-to-face meetings, and the post. Many respondents distinguished between 'secure' websites and websites in general, a judgment they made based on seeing a message announcing that they were accessing a secure web site, had noted a padlock symbol displayed on their browser window, or 'knew' to be secure. Individuals commonly said that one benefit of online interactions is that there is almost always a record of the event, and that they save a copy for future reference. In most groups, people expressed fear about "hackers," and repeatedly cited examples of stories from the media about different threats and vulnerabilities online The majority of participants maintained that they understand very little about what happens to information processed over the Internet, and those without much Internet experience tended to voice stronger fears about this channel compared to those with more experience.

While the phone was reported to be the least trusted channel for providing personal information, many individuals noted that the phone can help to preserve anonymity when seeking information from different organizations. Individuals in two different groups contended that the channel used to provide information is relatively insignificant, because the information is eventually stored on computers and subject to the same threats (most commonly noted in terms of "hackers getting into the databases"). As previously discussed, most individuals disagree with this contention, as they associate different risks and levels of confidence with each channel.

4.4 Data sharing

Asked about their views on the sharing of personal data or information between government agencies, a number of individuals reported that they believe data sharing programs are fundamentally breaches of information privacy, while others claimed that government data sharing programs contributed to a feeling of having little control over where their personal information is communicated. On the other hand, many expressed qualified support for certain data sharing arrangements, noting that there are situations where data sharing is necessary and acceptable, provided that two general conditions are met: the sharing is done fairly or ethically, and the individual perceives some

benefit as a result of the data sharing program. Many of these participants expressed frustration about having to submit the same information to different government organizations.

4.5 Emergent themes

One recurring theme that was central to most of the group discussions related to the unique context of the relationship between the State and its citizens. In contrast to the environment of the private sector, people reported feeling as though they have little power in this relationship, and little control over what information the State has about them and how it is used. Furthermore, individuals reported that they believe they have little or no choice about whether to provide personal information when a government organization requests it from them. Based on the comments made by participants and the frequency with which this topic occurred in the various discussions, this feeling of an uneven distribution of power seems to significantly influence the attitudes of the majority of these individuals.

Comments related to the technology itself reflected many different levels of knowledge about computers, the Internet, and technology in general (from inexperienced and uneducated/untrained, to experienced and educated/trained). Concerns were raised in relation to individuals' personal experiences and stories they had heard through various media channels, and centred around three themes: the security of computers and the Internet, increasing reliance on computers and information technology (including the perception of increased potential for privacy breaches), and a lack of understanding about what happens with personal information submitted to organizations.

In the discussions about the scenarios presented questions were asked about how certain events would impact on individuals' level of trust in the organizations involved. Two factors were commonly raised: the way the organization disciplines the employee(s) responsible for causing the breach, and the way the organization handles the situation with the individual whose privacy was breached. Both influenced the sense of grievance participants felt about the breach, and their future trust in the organization, regardless of the magnitude of the breach. Organizations which were open about the breach mitigated the extent to which trust would be withdrawn. Financial and health information remained the most serious areas in relation to breaches of privacy, causing most concern, and demanding redress from the organization concerned.

Finally, the researchers observed that some individuals' reported attitudes seemed to be contradicted by their reported behaviors. This occurred in more than one group, and was most often related to technology issues. While it may not be surprising that people's behaviors sometimes belie their reported attitudes and preferences, it is important to be aware of this when interpreting findings based on participants' reported attitudes. The use of scenarios, and a triangulated approach to the study was designed to minimise the impact of this phenomenon.

5. Discussion

A number of key issues emerge from this research. The first is the unique challenge facing government organizations based on their roles and responsibilities e.g., they must serve a wide variety of individuals, are often monopoly service providers, and many have the responsibility associated with compulsory data collection. A second relates to the diversity of reported perspectives as a reflection of the different attitudes, beliefs, feelings and experiences of the citizens served by the New Zealand Government. Although the questionnaire data was not analysed according to factors such as ethnicity, socio-economic status, and education, these issues did emerge in the group discussions. There are clear differences in the responses of Maori and Pacific cultural groups, and less fear of a breach of privacy in higher socioeconomic groups. This mirrors the findings of the Unisys surveys carried out in New Zealand and Australia in 2006 [38]. Suspicion of IRD and the social welfare agency WINZ may also be related to socio-economic status, as observed by Raab and Bennett [39].

There were also some very positive attitudes reported. Some participants acknowledged that using technology could potentially result in enhanced individual privacy. Interacting with government organizations via the Internet could allow individuals the autonomy to access government and submit information without the need to appear in person or discuss issues over the phone. There is also a substantial group of respondents who would be willing to supply information once, to one agency, to be shared across agencies, for the sake of convenience.

Concerns about the trustworthiness of government organizations were also influenced by the media, as much as by personal experience, and led to some perceptions that individuals have little control over the personal information they provide to government organizations, and generally lack power in their relationships with these organizations. There are a number of steps government agencies could take to mitigate these concerns, in particular explaining more clearly how information is stored, and who may have access to it. Existing statements on government web sites are more likely to refer to the use of names and addresses, or copyright and intellectual property issues. They rarely address concerns raised by citizens. Privacy statement on government web sites need to

communicate much better with citizens if they are to help build trust in e-government.

There is clearly a reminder here to government organizations to look to their privacy practices, develop policy and training programs related to privacy, information security, and trustworthy behavior at an individual as well as an organizational level in order to ensure that incidents labeled by citizens as 'incompetent' do not continue to occur. When breaches of privacy do occur, the consequences can be minimized by attention to the factors reported here-making clear the actions that have been taken to redress the issue in an open and honest way, in order to restore the trust that has been broken. This would also help to limit the impact of the breach to one agency, and prevent it from impacting on all government activity.

In conclusion, it seems that individuals have the most confidence in providing personal information in a face-to-face environment, and some confidence in the postal system. There is still widespread skepticism about privacy online. These attitudes are consistent with some of the findings from the recently published report, *Channel-Surfing: How New Zealanders access government*, which reports that the phone and the Internet are the two channels about which the majority oft New Zealanders have security concern [40]. These preferences appear to relate to the ability to form judgments about the trustworthiness of the individual to whom one is passing information, and the ability to build a relationship with that person, and the agency, they represent, however temporary that relationship is. It seems that a channel strategy that allows citizens choice in how they interact with government will be necessary for some time to come.

References

1. The New Zealand Government's effort to increase citizens' trust is identified in the "Development Goals" of the State Services Commission. Of these six goals, one is "Trusted State Services," with an objective of "Measurable improvement in New Zealanders' trust in the agencies of the State Services" by June of 2010 (4 December 2005, from: http://www.ssc.govt.nz/display/document.asp?docid=4730&pageno=3).

2. Westin, A. *Privacy and Freedom*. New York: Atheneum, 1967,p 7.

3. United Nations. *International Covenant on Civil and Political Rights, 1966.*. Retrieved 10 September 2005, from http://www.unhchr.ch/html/menu3/b/a_ccpr.htm

4. United Nations. *Universal Declaration of Human Right, 1948s*. Retrieved 10 September 2005, from http://www.un.org/Overview/rights.html

5. Schwartz, N. "Information at a price: Liberty vs. security." *Information Management Journal,* 37(3), 2003, p14.

6. Westin 1967, Nemati, H. Tao, W., & Gold, J "Understanding Tradeoffs: The link between knowledge and privacy concerns." *Proceedings of the 34th Annual Meeting of the Decision Sciences Institute Meeting, 2003.* .

7. Etzioni, A. *The Limits of Privacy*. New York: Basic Books, 1999. .

8. Westin,1967, p40..

9. Regan, P. *Legislating Privacy: Technology, Social Values and Public Policy*. Chapel Hill: University of North Carolina Press.,1995, p 221.

10. Hardin, R. *Trust and Trustworthiness* . New York: Russell Sage Foundation, 2003.

11. Rousseau, D. M., S.B. Sitkin, R.S , Burt and C. Camerer, "Not So Different After All: A cross-discipline view of trust." . *The Academy of Management Review*, 23(3),1988, 393–404., p395.

12. Soothill, W. E. *The Analects of Confucius*. New York: Paragon, 1968. (Original work published 1910).,

13. Council for Excellence in Government. *A Matter Of Trust: Americans and their Government 1958 – 2004.* Retrieved 5 May 2005, from http://www.excelgov.org/usermedia/images/uploads/PDFs/AMOT.pdf

14. Hardin, 2002, p151.

15. Bennett, C. J. and C.D. Raab, C. D. *The Governance of Privacy: Policy instruments in global perspective*. Hampshire, England: Ashgate,2003, p 49

16. Council for Excellence in Government. *The New E-Government Equation: Ease, engagement, privacy and protection,* 2003.. Retrieved 30 September 2005, from http://www.excelgov.org/usermedia/images/uploads/PDFs/egovpoll2003.pdf

17. Barnes, C. and D.Gill, "Declining Government Performance? Why Citizens Don't Trust Government." Working Paper, New Zealand State Services Commission, 2000.. Retrieved 12 October 2005, from http://www.ssc.govt.nz/display/document.asp?docid=2891

18. Transparency International. *Corruption Perceptions Index* 2005.. Retrieved 15 November 2005, from http://www.transparency.org/cpi/2005/cpi2005.sources.en.html

19. Dempsey, J.X., P.Anderson, and A. Schwartz. "Privacy and E-Government: A report to the United Nations Department of Economic and Social Affairs as background for the World Public Sector Report: E-Government." Center for Democracy and Technology. 2003. Retrieved 5 May 2005, from http://www.internetpolicy.net/privacy/20030523cdt.pdf p 1.

20. BeVier, L.R. "Information About Individuals in the Hands of Government: Some reflections on mechanisms for privacy protection." *William and Mary Bill of Rights Journal,* 4, 1995, 455-506., Prebble, M. *Information, Privacy and the Welfare State: an integrated approach to the administration of distribution.* Wellington: Victoria University of Wellington, Institute of Policy Studies, 1990. 1990).

21. Raab and Bennett, 1998, p264

22. Fukuyama, F. "Trust Still Counts in a Virtual World." *Forbes,Magazine*, 33-34, 1996. .

23 Friedman, B., P.H. Kahn and D.C. and Howe, "Trust Online" *Communications of the ACM* 43(12), 2000,p 40).

24. Solove, D.J. "A Taxonomy of Privacy." *George Washington University Public Law Research Paper* No. 129, 2005.. Retrieved 6 November 2005, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=667622.

25. Market and Opinion Research International. "Privacy and Data-Sharing: Survey of public awareness and perceptions."

2003. Retrieved 21 June 2005, from http://www.dca.gov.uk/majrep/rights/mori-survey.pdf

26. Unisys Asia Pacific. Unisys Security Index New Zealand: A Consumer Link survey, September Quarter 2006. Rhodes, NSW. Unisys., 2006.retrieved 9 September 2006 from http://www.unisys.com.au/services/security/security_confernce/index.html

27. Unisys Asia Pacific. Unisys Security and Survey Index. A Newspoll survey, September Quarter 2006. Rhodes, NSW. Unisys., 2006.retrieved 9 September 2006 from http://www.unisys.com.au/services/security/security_confernce/index.html

28. *GO2003 Government Online, a National Perspective 2003 - New Zealand.* Taylor Nelson Sofres , Retrieved 19 May 2006 from: http://www.e.govt.nz/resources/research/go-survey-2003

29 Council for Excellence in Government. *The New E-Government Equation: Ease, engagement, privacy and protection*. 2003. Retrieved 30 September 2005, from http://www.excelgov.org/usermedia/images/uploads/PDFs/egovpoll2003.pdf.

30. Booz Allen Hamilton. *Beyond e-Government: The world's most successful technology-enabled transformations.*2005. Commissioned by the United Kingdom Presidency of the European Council. Retrieved 19 December 2005, from http://www.egov2005conference.gov.uk/documents/pdfs/beyond_egov.pdf, 24-25, p14.

31. Cullen, R. and P. Hernon, P. *Wired For Well-Being: Citizens' Response to E-Government*. Report to the E-Government Unit of the State Services Commission.Wellington: State Services Commission, 2004. Retrieved 2 December 2005, from http://www.e.govt.nz/resources/research/vuw-report-200406

32. Smith, H.J., S.J.Milberg, and S.J.Burke."Information Privacy: Measuring individuals' concerns about organizational practices." *MIS Quarterly,* 20(2), 1996, p167.

33. Dinev, T. and P. Hart. "Internet Privacy Concerns and Their Antecedents – Measurement validity and a regression model." *Behaviour and Information Technology*, 23 (6), 2004, pp 413 – 422.

34. Hu, Q. and T. Dinev. "Is Spyware an Internet Nuisance or Public Menace." *Communications of the ACM*, 48(8), 2005, pp61-66., p65.

35. Bellman, S., E.J.ohnson, S.J. Kobrin, and G.L. Lohse,. "International differences in information privacy concerns: a global survey of consumers." *The Information Society*, 20, 2004,pp313-324.

36. Reilly, P and R. Cullen. *Information Privacy and Trust in Government: a citizen-based perspective.* Wellington: State Services Commission, 2006. Retrieved 16 January 2006 from: http://www.e.govt.nz/resources/research/trust-and-privacy

37. *GO 2003.*

38. Unisys Asia Pacific. Unisys Security Index New Zealand: A Consumer Link survey, September Quarter 2006. Rhodes, NSW. Unisys., 2006.retrieved 9 September 2006 from http://www.unisys.com.au/services/security/security_confernce/index.html

39. Raab and Bennett, 1998, p264.

40.Curtis, C. J. Vowles, and B. Curtis. *Channel-Surfing: How New Zealanders Access Government*. Wellington, State Services Commission, 2004. Retrieved 5 May 2006, from http://www.e.govt.nz/resources/research/channel-surfing-200409