

Information Privacy and Trust in Government: A citizen-based perspective

Patrick Reilly
2005 Fulbright Fellow

Rowena Cullen
Associate Professor
School of Information Management
Victoria University of Wellington

A report presented to the State Services Commission

January 2006

CONTENTS

EXECUTIVE SUMMARY	3
1 Introduction	5
2 Literature Review	7
2.1 INTRODUCTION AND BACKGROUND	7
2.1.1 The Need for Balance	7
2.1.2 “Trust in Government”	8
2.2 GOVERNMENT & CITIZENS’ PERSONAL INFORMATION.....	9
2.3 INTERNATIONAL CONTEXT: REGULATING PRIVACY	11
2.4 PRIVACY AND TECHNOLOGY	11
2.5 OTHER FACTORS INFLUENCING PRIVACY CONCERNS	12
2.5.1 Culture and National Privacy Regulation	12
2.5.2 The Influence of Media Content	13
2.5.3 Legislative Reactions to Terrorism.....	13
2.6 CHALLENGES RELATED TO RESEARCHING PRIVACY	13
2.7 PRIVACY & TRUST ONLINE	14
2.7.1 E-Commerce Research.....	15
2.8 E-GOVERNMENT, INFORMATION PRIVACY AND TRUST.....	16
3 Methodology.....	18
3.1 FOCUS GROUP INTERVIEWS WITH COMMUNITY GROUPS	18
3.2 SURVEY OF INDIVIDUALS REPORTING PRIVACY COMPLAINTS	19
3.3 INTERVIEWS WITH COMMUNITY LEADERS / REPRESENTATIVES.....	20
3.4 SYSTEMATIC ANALYSIS OF QUALITATIVE DATA.....	21
4 Findings	22
4.1 FOCUS GROUPS – QUESTIONNAIRE DATA.....	22
4.1.1 Background Data	22
4.1.2 Concerns, Attitudes and Behaviors (prior to discussion).....	24
4.2 FOCUS GROUPS – DATA FROM DISCUSSIONS.....	27
4.2.1 Defining Privacy and Gauging Awareness	27
4.2.2 The Trustworthiness of Government Organizations.....	28
4.2.3 Prevailing Themes and Recurring Topics.....	34
4.3 SURVEY OF COMPLAINANTS TO THE OPC	41
4.3.1 Reported Level of Trust: Before and After	41
4.3.2 Willingness to Provide Personal Information	42
4.4 INTERVIEWS WITH COMMUNITY LEADERS / REPRESENTATIVES.....	44
4.4.1 Interview #1: Social welfare beneficiaries.....	44
4.4.2 Interview #2: Ethnic councils in New Zealand.....	45
4.4.3 Interview #3: Pacific peoples.....	45
4.4.4 Interview #4: Maori	46
4.4.5 Interview #5: Muslims	48
4.4.6 Interview #6: People with disabilities.....	48
4.4.7 Interview #7: Women	49
4.4.8 Interview #8: Older New Zealanders.....	50
5 Discussion	52
5.1 CONCERNS ABOUT INFORMATION PRIVACY	52
5.2 AWARENESS OF PRIVACY PROTECTIONS / REGULATIONS	54

5.3 HOW TRUSTWORTHY ARE GOVERNMENT ORGANIZATIONS?	55
5.4 WHAT HAPPENS TO TRUST WHEN PRIVACY IS VIOLATED?.....	56
5.5 DO THE CONSEQUENCES OF A BREACH PROPAGATE?	57
5.6 CONFIDENCE IN CHANNELS:.....	57
F. Conclusion	59
REFERENCES	62
APPENDIX A: Focus Group Questionnaire.....	67
APPENDIX B: Focus Group Scenarios.....	69
APPENDIX C: Survey of Complainants.....	70
APPENDIX D: Protocol for Conducting Survey of Complainants.....	73
APPENDIX E: Interview Questions (Group Representatives)	74
APPENDIX F: Coding Framework	76

TABLES

Table 1. Focus group participants - Gender.....	22
Table 2. Focus group participants - Age.....	22
Table 3. Focus group participants - Use of online services	22
Table 4. Reported attitudes, concerns and behaviors.....	24
Table 5. Levels of trust in different government organizations.....	25
Table 6. <i>Most</i> trusted government organizations	26
Table 7. <i>Least</i> trusted government organizations	26
Table 8. Comments: The power of government organizations.....	34
Table 9. Comments: General security and privacy concerns related to the Internet	35
Table 10. Comments: Concerns about the insecurity of personal information.....	36
Table 11. Comments: Concerns from experienced and educated users.....	37
Table 12. Comments: The influence of punishment.....	38
Table 13. Trust in organizations, before and after incident	41
Table 14. Willingness to provide information, attitudes and behavior.....	43

“Information supplied by citizens to government is the indispensable handmaiden of the modern activist state” – Lillian R. BeVier, 1995

EXECUTIVE SUMMARY

Throughout the world, countries are facing the challenges associated with protecting citizens’ information privacy while working to realize the potential of electronic government. While many of these governments are also striving to increase citizens’ trust and confidence, technology and innovation continue to change the way individuals’ personal information is collected, correlated, processed, communicated and traded as a valuable commodity. The literature in these areas gives evidence to the important and complicated roles that privacy and trust play in contemporary relationships, especially in interactions taking place in the online environment.

In order to learn how New Zealanders’ experiences with, and concerns related to, information privacy affect the amount of trust they place in government organizations, three research projects collected data from New Zealanders: a series of eight focus groups comprising a variety of community groups, a survey of individuals who had submitted privacy-related complaints to the Office of the Privacy Commissioner, and a series of eight interviews with community representatives. The resulting data sets reflected a diverse range of attitudes about issues related to information privacy and the trustworthiness of government organizations.

The main findings of this study were:

- Participants’ concerns about information privacy fell within two main categories: technology-related concerns (including the perception that there is greater potential for damaging privacy breaches, plus worries more closely associated with the Internet), and concerns specifically related to government organizations (including uncertainty about the training and competence of public servants, as well as concerns about the sharing of citizens’ personal information among government organizations). While media stories were reported to be the primary cause of technology-related privacy concerns, worries about government organizations were more often the result of personal experiences and stories from family and friends.
- The majority of participants were unaware of their rights in relation to information privacy, were unlikely to be aware of the Privacy Act of 1993 (unless they dealt with this Act based on their occupation), and were largely unfamiliar with the obligations placed on organizations that request and collect their personal information.
- When providing personal information to government organizations, participants had the greatest confidence that their privacy would be protected if they provide their information in a face-to-face environment, followed by the post and then the Internet, with the least amount of confidence in the telephone. Participants reported that the most important confidence-promoting properties of channels were: some form of

interaction with the recipient of the information (relationship), the ability to retain a record of the interaction, the ability to check the accuracy of the information being submitted, and the ability to understand how information is delivered to the destination.

- Although nearly all participants reported having low levels of confidence in the privacy and security of the Internet, many continue to use online services (e.g., online banking, electronic commerce websites, and online auction websites). Convenience was the most commonly cited benefit of using online services.
- The majority of participants reported having greater confidence that their privacy will be protected by government organizations in comparison to organizations that are not government. This was most often based on their perceptions about the objectives, motivations, transparency and accountability associated with government organizations.
- In discussing their attitudes towards government organizations, many participants emphasized that they believe they have little power in the relationships they have with these organizations (in contrast to their relationships with private businesses). This imbalance of power was said to contribute to beliefs that they have little control over what information government organizations have about them, and how their personal information is used.
- Most participants reported that they assess the trustworthiness of each government organization separately, and therefore, they trust some more than others. The factors that most significantly influenced individuals' assessment of organizational trustworthiness were: their personal experiences with the organization (and the resulting relationship), stories from family and friends, and stories from various media channels.
- In most cases, breaches of privacy appear to have an adverse effect on individuals' trust in the offending organization. While the majority of survey respondents reported that a breach by one government organization had diminished the amount of trust they had in government organizations in general, most focus group participants reported that a breach would only affect their attitude toward the offending organization. The factors most influential in determining the effect that a breach of privacy would have on trust related to: the perceived cause of the breach, the sensitivity of the information involved, the type of breach (e.g., improper disclosure), and the way the offending organization handled the situation.

In conclusion, government organizations are encouraged to ensure that privacy principles stated on their websites include information about how personal information is managed and protected when it is being requested for official purposes, as well as in the monitoring of website activity, while also ensuring that policies related to information privacy are well understood and observed by employees. A new model of communication between citizens and government organizations is needed in the e-government environment to ensure that citizens are able to maintain meaningful relationships with government organizations and develop trust in their interactions with these organizations through the Internet. This new model, based on ongoing research in

the field, will better represent the necessary balance between the power of the state, and the empowerment of the individual which e-government claims to foster, and may help to promote citizens' confidence in the trustworthiness of government organizations.

1 Introduction

The purpose of this study was to investigate the relationship between privacy and trust, with emphasis on how citizens' concerns about, and experiences involving, information privacy are related to the level of trust they have in government organizations. In addition to being an important component of social interactions in general, trust, or rather the perception of being trustworthy, is seen as an integral resource for the governments of modern democratic states. From a citizen's perspective, in addition to promoting personal autonomy and dignity, the right to privacy is arguably one of the fundamental tenets of liberal democracy.

Throughout the world, information and communications technologies are changing the way governments operate and interact with citizens, as part of a shift towards what is commonly called 'electronic government.'¹ These technologies have also changed, and will continue to change, the way individuals' information is collected, communicated, processed and stored, while a number of factors are making personal information more readily available than ever before.

Additional investigation of the relationship between citizens' perceptions about information privacy and their trust in government should advance our understanding of the roles they play in the operation of modern democratic systems. These issues have global relevance, and this research was conducted in New Zealand, one of many countries facing the challenges associated with increasing citizens' trust in government.²

This study sought to explore a number of research questions, including:

1. What are New Zealanders' concerns about their informational privacy?
 - a. What influences these concerns?
 - b. To what extent are people aware of the protections that exist to protect their right to privacy?
 - c. To what extent are people aware of the available options for recourse if they believe their privacy has been breached?

¹ According to the Organization for Economic Co-operation and Development (OECD), e-government involves "*the use of information and communication technologies, and particularly the Internet, as a tool to achieve better government*" (Retrieved 5 Dec 2005, from: [http://webdomino1.oecd.org/COMNET/PUM/egovproweb.nsf/viewHtml/index/\\$FILE/glossary.htm](http://webdomino1.oecd.org/COMNET/PUM/egovproweb.nsf/viewHtml/index/$FILE/glossary.htm)).

² 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. How trustworthy do New Zealanders believe government organizations are in relation to protecting their information privacy?
3. When an individual believes an organization has violated their privacy, does this have an impact on that individual's level of trust in that organization?
 - a. What is the magnitude of this relationship?
 - b. What factors influence the magnitude of the impact (if any)?
4. If one government organization breaches an individual's privacy, does this affect the individual's perception of the trustworthiness of only that specific organization, or 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.
 - a. What influences the level of confidence people have?
 - b. What are New Zealanders' attitudes towards, and concerns about, using the Internet to communicate personal information?

In order to collect data and information from a variety of New Zealanders, three different projects were conducted, each using a different method of data collection to gather input from different populations.

This report explains how the research was conducted and discusses the results of the study. First, a review of the literature relevant to this study is presented to introduce many of the topics involved in this area of research. Then, the methodology that the research team followed is described. Next, the data collected in each of the three projects is put forth in the "Findings" section. Then, a discussion of these findings is presented, focusing on the potential implications of the collective results of the three projects. Finally, a series of recommendations are provided in the conclusion of this report.

2 Literature Review

This section presents a review of the literature relevant to this study. Given the vast quantity of research and scholarly writing on the subjects involved, emphasis is focused on those areas most central to the scope of this research.

2.1 INTRODUCTION AND BACKGROUND

In any meaningful discussion of privacy, it is important to clarify what is meant by the term privacy. In one of the most influential articles on this subject, “The Right to Privacy,” Samuel Warren and Louis Brandeis articulated their argument for the importance of individual privacy and described the right as one’s “right to be let alone” (1890, 193). In addition to the many different definitions that have been put forth, several commentators have offered classifications of the various dimensions of privacy, (Prosser 1960,³ Westin 1967⁴ and Solove 2005,⁵ among others) attempting to bring clarity to its seemingly myriad interpretations. 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” (Westin 1967, 7).

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” (United Nations [UN], 1966). Similar protections are also supported in Article 12 of the *Universal Declaration of Human Rights* (UN, 1948).

2.1.1 The Need for Balance

Scholars have claimed that privacy is a necessary requirement for life in modern democratic states (Warren & Brandeis 1890, Westin 1967, Dempsey, Anderson, & Schwartz 2003), and that it contributes to an individual’s personal autonomy and dignity. At the same time, there is general agreement that privacy is not an absolute right. For example, it is often argued that (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

³ Based on American legal cases, Prosser’s 1960 article “Privacy,” classifies privacy torts into four distinct categories.

⁴ In addition to articulating “four basic states of individual privacy,” Westin also proposes that the four primary functions of individual privacy are “personal autonomy, emotional release, self-evaluation, and limited and protected communication,” and notes that “...these four functions constantly flow into one another” (31).

⁵ In “A Taxonomy of Privacy,” Solove presents a contemporary classification of the various “activities that impinge upon privacy” (3), including comment on the threats to privacy that have been created by technological developments. The four general categories of harmful activities in Solove’s taxonomy are: information collection, information processing, information dissemination, and invasion (8).

these seemingly competing interests (Westin 1967, Nemati, Tao & Gold 2003). This need for balance has led to longstanding discussions and controversy about how to assess the value of these interests and accordingly, how to determine what is a “reasonable” trade-off. For example, in *The Limits of Privacy*, contemporary scholar Amitai 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 (1999). Despite the competing philosophies about how decisions should be made to promote a balance, Westin notes, “either too much or too little privacy can create imbalances which seriously jeopardize the individual’s well-being” (1967, 40). In addition to this view of personal privacy, other commentators have suggested that the value of privacy may not be limited to the individual level, but may also have “common, public, and collective purposes” (Regan 1995, 221).

Similar to privacy, the notion of trust has been the focus of considerable academic debate and disagreement throughout a variety of fields.⁶ Despite differing theories about how trust is engendered and maintained⁷ there appears to be 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” (Rousseau, Sitkin, Burt, & Camerer 1998, 395).

2.1.2 “Trust in Government”

In various political systems throughout the world, it is claimed that citizens’ trust in government is valuable and enabling. 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” (Soothill 1968, 571-72).⁸ Contemporary research suggests that, in modern democracies, citizens’ distrust of their government may have an adverse effect on the effectiveness of that government (Council for Excellence in Government, 2004).

Given the scope of this study, it is important to acknowledge that the concept of a citizen’s “trust in government” is distinctly different from interpersonal trust. A person saying that they trust another specific individual (for instance, a colleague) carries different connotations than an individual saying “I trust the government.” While the former would be about interpersonal trust, as an assertion about the speaker’s assessment of the trustworthiness of their colleague, the latter is seemingly a generalization about the speaker’s perception of the collective trustworthiness of the many different organizations

⁶ Including but not limited to: philosophy, psychology, sociology, economics, information systems, management, public policy and political science.

⁷ Russell Hardin provides comment on aspects of four dominant theories of trust: encapsulated interest, commitment from character, dispositional trust, and moral commitment in *Trust and Trustworthiness* (2003).

⁸ Some translations of *The Analects* use the word “trust” directly, others paraphrase trust as in “confidence of the people” and a people’s “faith in their rulers” (Soothill, 1968). Specifically, this idea comes from *The Analects of Confucius*, and was referred to by Professor Onora O’Neill in *A Question of Trust* (2002).

that comprise the government (where there can be many different views on which entities are part of ‘the government’).

One’s ability to assess the trustworthiness of an organization is related to his or her expectations and knowledge of that organization (including the intentions and competence of the individuals who may be involved in any interaction that he or she has with the organization). Given that governments are comprised of thousands of individuals⁹ working in hundreds of organizations, a citizen’s attempt to evaluate the trustworthiness of their government may be considered a formidable challenge. In his book *Trust and Trustworthiness*, 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” (2002, 151).

Despite this claim, as Bennett and Raab observe in *The Governance of Privacy*, “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” (2003, 49). While a number of competing theories attempt to identify the factors that most significantly influence citizens’ trust in government,¹⁰ there are significant gaps in our knowledge about how to effectively promote and maintain the public’s trust in government.

In the United States (U.S.), research studies indicate that Americans’ level of trust in their government has decreased significantly since the early 1970s (Council for Excellence in Government, 2004). 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 (Barnes & Gill, 2000). This apparent decline in public trust has occurred despite New Zealand’s consistently high rankings in Transparency International’s *Corruption Perceptions Index* (CPI), which ranks the country’s government amongst the least corrupt in the world (Transparency International, 2005).¹¹

2.2 GOVERNMENT & CITIZENS’ PERSONAL INFORMATION

Government organizations comprise an important part of the unique relationship between citizens and the state, and this affects the responsibilities of these organizations with

⁹ Or even millions, as is the case in the US.

¹⁰ For example, in the Council for Excellence in Government’s 2004 report, *A Matter of Trust: Americans and their Government 1958 - 2004*, the authors discuss five popular theories based on: 1. Presidential approval and economic conditions, 2. Mood of the nation, 3. External threats, 4. The media, and 5. Trust in people (6-11).

¹¹ Out of 159 countries, New Zealand was tied with Finland for the second best ranking in the 2005 CPI (behind Iceland), and has been ranked amongst the top four countries for the past five years. According to Transparency International, the CPI “relates to perceptions of the degree of corruption as seen by business people and country analysts.”

respect to protecting the privacy of individuals' information. In contrast to private businesses that market goods and services to customers, government organizations have a responsibility to serve a very diverse set of individuals, including those with different needs, beliefs, attitudes, cultures, languages and educational levels (Kent & Millett, 2003). Furthermore, within the operations of most governments, various requests for personal information are supported by governmental mandates (Bennett & Raab 2003, BeVier 1995). Thus, in some situations, the provision of personal information to government organizations is compulsory. This sharply contrasts the nature of information exchanges that individuals engage in with private organizations, where it may be argued that individuals make conscious decisions about which organizations they choose to provide their personal details to. In their report to the United Nations entitled "Privacy and E-Government," Dempsey, Anderson, and Schwartz clarify the point that "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" (2003, 1). In light of the relevance of this unique relationship between government and citizen, this topic will be explored further in later sections of this report.

Governments collect personal information from citizens for many purposes, for instance determining appropriate taxation and the provision of social welfare benefits. The collection of information in these interactions, wherein citizens provides information about themselves to a government organization, is justified based on the requirements of the specific interaction (commonly involving a need to establish or verify an individual's identity). Looking at a specific example, the procedures designed to facilitate the redistribution of resources within welfare states (i.e., social welfare programs) require benefit applicants to provide detailed personal information in order to determine their eligibility for beneficiary status (BeVier 1995, Prebble 1990). This requirement is logically reasonable, as the decision-making process requires detailed information about each applicant, often including financial and health-related information. The implicit sensitivity of this information may further emphasize the importance of ensuring that the information is handled properly and used only for the purpose it is collected for.

Since individuals in lower socioeconomic groups are typically thought to be more reliant on government programs (e.g., more likely to provide information to welfare programs, etc.) it is often suggested that these sections of the population are more susceptible to invasions of their privacy. However, based on their investigation of the distribution of privacy risks throughout society, Raab and Bennett (1998) 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" (264).

2.3 INTERNATIONAL CONTEXT: REGULATING PRIVACY

A review of international privacy laws reflects the range of disparate regulatory approaches taken by various governments to protect citizens' privacy. Although many countries (including the European Union (UN), New Zealand, and Australia) have based their privacy regulations on the Organization for Economic Cooperation and Development's (OECD) *Guidelines Governing the Protection of Privacy and Transborder Data Flow of Personal Data* (1980), subsequent decisions about implementation and development of domestic policies have resulted in divergence amongst these countries. Thorough comparisons of these regulations exist (Klosek 2000,¹² Koppe 2002¹³), including the Electronic Privacy Information Center (EPIC) and Privacy International's report *Privacy and Human Rights 2004: An international survey of privacy laws and developments*, which provides analysis of privacy regulations in over sixty countries, including the U.S. and New Zealand.

The approach to privacy regulation in the U.S. is markedly different from that of New Zealand. American regulation is not based on the OECD's "Guidelines," but rather derives from the *Fair Information Practices*, developed by the U.S. Department of Health, Education and Welfare (HEW) in 1973. Instead of a comprehensive regulatory approach (like those of the European Union,¹⁴ New Zealand,¹⁵ and Australia¹⁶), the U.S.'s sectoral approach has resulted in the development of different privacy codes for various areas (e.g., the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Family Educational Rights and Privacy Act (FERPA), the Fair Credit Reporting Act (FCRA), Electronic Communications Privacy Act of 1986 (ECPA), among others). This "patchwork of federal laws" and self-regulation (EPIC and Privacy International, 2004) has been criticized in comparison to other models of comprehensive legislation and regulation (Koppe, 2002).

2.4 PRIVACY AND TECHNOLOGY

Given that privacy issues are fundamentally related to the society in which an individual lives (Moore 1984,¹⁷ Milberg, Smith, & Burke 2000), it is no surprise that these issues tend to be influenced by changes in society, especially changes involving the use of technology. For example, when Warren and Brandeis addressed the issue in 1890, their writing acknowledged the privacy-related implications of advances in communications, photography, and printing. Based on our inability to reliably predict future technological

¹² Klosek compares privacy legislation in the United States and European Union, including analysis of the legislation of fifteen members states of the EU.

¹³ Koppe compares data protection in the EU, the US, and New Zealand, with emphasis on Internet privacy.

¹⁴ The European Union's European Union Data Protection Directive (1995)

¹⁵ New Zealand's Privacy Act of 1993

¹⁶ Australia's Privacy Act 1988

¹⁷ Specifically, Moore notes that the "need for privacy is a socially constructed need. Without society there would be no need for privacy" (1984, 73).

developments and innovations (much less, their consequences), privacy regulations are often established as a reaction to new threats (Bennett & Raab 2003, Langenderfer & Cook 2004).

Increasing concern regarding the perceived reduction of personal privacy in the Information Age is a consistent theme in the literature of various fields. The ubiquity of computers, communications networks, and digital information has created an environment in which personal details are arguably more readily available than ever before. In “A Taxonomy of Privacy,” Daniel Solove speaks to this concept as he describes modern “architectural problems” related to privacy, which involve “the creation of the risk that a person might be harmed in the future” (2005, 7). Solove observes that “the general progression from information collection to processing to dissemination is the data moving further and further away from the control of the individual” (8), which may be related to increases in the level of public concern about privacy. Other research supports the claim that individuals’ privacy concerns are related to perceptions that they do not have control over their personal information (Market and Opinion Research International [MORI], 2003).¹⁸

2.5 OTHER FACTORS INFLUENCING PRIVACY CONCERNS

2.5.1 Culture and National Privacy Regulation

Scholars have acknowledged the important relationship between a people’s culture and their valuation and interpretation of privacy, as historical events and traditions shape values and expectations (Westin, 1967). The influential role culture plays in shaping privacy concerns has been corroborated by cross-cultural research studies (Milberg, et al. 2000, Bellman, Johnson, Kobrin, & Lohse 2004). For example, Dinev, Belloto, Hart, Colautti, Russo, and Serra compare the privacy concerns of individuals in Italy and the U.S. with respect to factors including citizens’ “propensity to trust” and the individualistic or collectivist nature of each culture (2005).

The findings of multiple research studies indicate that the manner in which a country regulates information privacy may be related to the privacy-related concerns of its citizens (Milberg, Burke, Smith, & Kallman 1995, Milberg et al. 2000, Bellman et al. 2004). Milberg et al. (1995) found that citizens of countries that have more moderate approaches to regulating information privacy have more moderate levels of concern, while individuals in jurisdictions where there is either no regulation or very strict privacy regulation tend to report considerably lower levels of concern about information privacy. In light of the significant differences in the approaches to privacy regulation in the U.S. and New Zealand (in addition to important cultural differences), it is likely that the

¹⁸ Findings of this study are based on a survey of individuals in Great Britain and Northern Ireland.

citizens of these countries have different privacy-related concerns and different levels of sensitivity related to various issues.

2.5.2 The Influence of Media Content

Throughout the world, recent events (e.g., widely publicized data breaches involving ChoicePoint, Bank of America, and Lexis-Nexis, among many others), technological developments (use of biometrics, surveillance, Internet tracking, radio-frequency identification), and political issues (proposals for national identification cards, the creation of public registers and unique identifiers) have resulted in much attention being focused on issues of privacy.¹⁹ The increasing frequency of privacy-related issues in popular media has been postulated as one of many factors contributing to public anxiety about threats to individual privacy (Raab & Bennett, 1998).

2.5.3 Legislative Reactions to Terrorism

In the past five years, several countries have taken legislative actions in response to the perceived threats of terrorism (e.g., in the U.S., the USA PATRIOT Act,²⁰ other measures have been taken in the UK, Australia and other jurisdictions). It has been argued that a number of anti-terrorism measures have involved the forfeiture of personal privacy in exchange for security (EPIC and Privacy International, 2004). If individuals believe privacy protections have been reduced, this may affect individuals' associated concerns. Reflecting this global trend, the literature includes analysis of the corresponding impacts on civil liberties and human rights, including individual privacy (Taylor 2003, Swartz 2003, Kerber & Thomas 2003, Nelson 2004).

2.6 CHALLENGES RELATED TO RESEARCHING PRIVACY

Based on the complexity of individuals' attitudes towards privacy, any research being conducted with the objective of shedding light on privacy issues must be carefully designed and implemented. It is challenging to obtain a meaningful, objective snapshot of public opinion, especially on a subject with such a multitude of interpretations (i.e., since researchers and scholars have been unable to agree on a definition of privacy, it is reasonable to expect that the public may not be entirely sure about how to interpret a poorly designed survey question about privacy). Many quantitative surveys have asked general questions about "how concerned" individuals are about privacy, yet these simple questionnaires often fail to explain the nature of these concerns or identify the associated causes (Smith, Milberg & Burke, 1996).

¹⁹ The EPIC website provides comment on these privacy-related issues (including publicized breaches, technology, politics and more) at <http://www.epic.org/privacy/> (14 Nov 2005).

²⁰ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, available from <http://thomas.loc.gov/cgi-bin/bdquery/z?d107:h.r.03162>: (Retrieved 29 Nov 2005).

Since statistics derived from public opinion surveys are often used to inform and influence the development of important public policies, the quality of research design and objectivity of questioning is paramount. In his article “Public Opinion Surveys and the Formation of Privacy Policy,” researcher Oscar Gandy Jr. discusses problems of framing survey questions about privacy and affirms, “policy advocates continue to introduce strategic representations of public opinion into the policy process” (2003, 296). Specifically, the objectivity of many large research surveys have been questioned based on the framing of questions and the motivations of those funding the research (Gandy 2003, Electronic Privacy Information Center [EPIC] 2005). For example, long-time privacy researcher Alan Westin’s survey findings on public opinion about privacy-related issues are often cited throughout the world. In the past five years, multiple commentators have questioned the objectivity of Westin’s surveys, including a pattern that EPIC refers to as “strong correlations between the conclusions of Mr. Westin’s studies and the interests of the companies sponsoring them” (EPIC, “Public Opinion on Privacy”).

Moreover, although survey research can provide some indication of public opinion and attitudes, multiple research findings indicate that individuals’ behaviors may directly contradict their declared privacy preferences or attitudes towards privacy (Spiekermann, Grossklags & Berendt 2001, Nemati et al. 2003).

2.7 PRIVACY & TRUST ONLINE

Renowned scholar Francis Fukuyama, has emphasized the important role trust plays in interactions and relationships involving the Internet (1996). This intuitive and commonly accepted idea is 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” (2000, 40).

A survey of the literature reveals that many researchers have begun to investigate dimensions of privacy in relation to use of the Internet. A report published by the Pew Internet and American Life Project in 2000 indicates low levels of understanding related to online privacy issues, as 56 percent of American Internet users were unaware that cookies were used to track their online activities.²¹ The report concludes that individuals are increasingly concerned about privacy-related issues, and although “Internet users express considerable fears about... problems they might face online... they behave in surprisingly trusting ways in many sensitive online areas” (Fox, Rainie, Horrigan, Lenhart, Spooner, & Carter, 12). A recently released survey of Internet users in the U.S. reports that 53 percent of this group “say they have stopped giving out personal information on the Internet” (18) and that the most important factor influencing their

²¹ A cookie is a text file (sent to a user from a web server) stored on a user’s computer, which are commonly used to help websites track users online.

decisions to visit a web site is that “the site will keep personal information I provide safe and secure” (Consumer Reports 2005, 9). Research specifically focused on gauging New Zealanders’ views about interacting with government online suggests that, in comparison to thirty other countries, New Zealanders have an above average “perception of ‘safety’ in providing personal information to Government over the Internet.” The same research suggests that this perception of safety has increased considerably among some groups of New Zealanders who use government online (Taylor Nelson Sofres, 2003).²²

In addition to general quantitative surveys, researchers have contributed to our understanding of the antecedents of users’ online privacy concerns. The associated findings suggest that an individual’s privacy concerns are directly related to one’s perceived vulnerability, and also highlight the complicated role of one’s perceived ability to exercise control over their own information (Dinev & Hart 2004).²³ Hu and Dinev suggest 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 (2005, 65). 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 (Bellman et al. 2004).

2.7.1 E-Commerce Research

Many researchers have studied the importance of privacy in the developing field of electronic commerce (e-commerce). Commentators suggest that individuals are increasingly aware that personal information is a valuable commodity to others, and are also sensitive about the associated risks (Olivero & Lunt, 2004). The findings of Liu, Marchewka, Lu & Yu, suggest that dimensions of privacy have “a strong influence on whether an individual trusts an [e-commerce] business” and this “will influence their behavioral intentions” to use an e-commerce website (2005, 300). Although the context of transactions in the public sector differs greatly from that of the private sector, this general concept may also apply to citizens’ use of government online. In a study that investigated individuals’ privacy preferences (and concerns) and then observed individuals’ actions in an online shopping experiment, the observed behavior was shown to be “in sharp contrast to their self-reported privacy attitude” (Spiekermann et al. 2001, 14). This may indicate a lack of understanding about the privacy-related implications of online activities.

Although this body of e-commerce research provides a number of conclusions related to this study, the nature of relationships within the ‘customer – business’ model of commercial business transactions is fundamentally different from those within the ‘citizen – state’ model of liberal democracies. Among other differences, distributions of

²² Specifically, the report finds, “The perception of safety in providing personal information to Government over the Internet increased significantly among a number of [government online] user groups...” (Retrieved 2 December 2005, from: <http://www.e.govt.nz/resources/research/go-survey-2003/chapter1.html>)

²³ As the authors note, their findings indicate that the relationship between one’s ability to control information and their privacy concerns was not statistically significant, and they present several reasonable explanations for this seemingly counter-intuitive result.

power among the parties of these transactions are notably dissimilar, as previously discussed. Therefore, while it is important to be aware of these findings and consider their implications, it is seemingly illogical to presume that they can simply be extrapolated to cover interactions within the public sector.

2.8 E-GOVERNMENT, INFORMATION PRIVACY AND TRUST

The governments of New Zealand and the U.S. have invested (and continue to invest) large amounts of money into their respective e-government efforts. The proposed benefits of e-government commonly include improved performance of government organizations and improved service delivery to citizens.²⁴ Although the governments of both New Zealand and the U.S. have been using computers to process citizens' personal information for decades, their increasing use of information and communications technology (especially the Internet) has affected the way citizens' personal information flows to, from and within each government.

Internationally, research indicates that 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 similar proportions of the population also have concerns about the privacy and security of their personal information submitted through government websites (Council for Excellence in Government, 2003). Research commissioned by the United Kingdom Presidency of the European Council has investigated the current status of, and challenges facing, e-government efforts in Australia, Canada, France, Germany, Italy, Japan, Sweden, the U.K., and the U.S. This research proposes that “*all countries face the same challenges of balancing information privacy against potential service enhancements,*” including the need to protect citizens' privacy while satisfying the authentication requirements of government online (Booz Allen Hamilton 2005, 24-25). The 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*” (14).

Research from New Zealand reflects similar privacy issues related to citizens' perceptions about how government organizations handle their information, and the effect these issues have on their confidence in government. In *Wired For Well-Being: Citizens' response to e-government*, Cullen and Hernon (2004) provide a general overview of New Zealanders' trust in government and perceptions about government websites. Based on focus group research, these findings suggest that citizens have greater confidence in government websites compared to websites in general, and that privacy and security

²⁴ For example, from <http://www.e.govt.nz/about-egovt>: “[E-Government] enables government agencies to separately and collectively lift their performance and deliver better results...” and “E-government makes the best of [government] investment to deliver improved services to New Zealanders.” (20 Dec 2005).

issues were sources of concern amongst those who participated. This report also indicates that individuals believed they had little control over their personal information, and expressed the view that government data sharing activities could potentially reduce their confidence in government organizations. *Channel Surfing: How New Zealanders Access Government* presents the results of a telephone-based, quantitative survey, which indicate that the phone and the Internet are the two channels that the most New Zealanders have security concerns about (Curtis, Vowels & Curtis 2004, 7)

The strategic plans of the New Zealand and U.S. Governments appear to rely heavily upon the use of the Internet and other information and communications technologies.²⁵ In light of this, it is important for each to learn about how they can successfully respond to this challenge of maintaining a balance between protecting citizens' privacy and realizing the potential benefits of e-government.

²⁵ As of December 2005, evidence of these strategic views is available at <http://www.e.govt.nz/about-egovt/strategy> for N.Z. and http://www.firstgov.gov/Topics/Includes/Reference/egov_strategy.pdf for the U.S.

3 Methodology

This study used three instruments for collecting information from different groups of New Zealanders. A series of eight²⁶ focus groups were held in and around the Wellington region, with an average group size of seven individuals. Also, a series of semi-structured interviews were conducted with individual representatives of specific groups of New Zealanders. Another section of the New Zealand population that was identified as having valuable information to contribute to this research consists of those individuals who believe that their privacy has been breached. Therefore, a survey questionnaire was designed and used to collect information from those individuals who have submitted privacy-related complaints to the Office of the Privacy Commissioner (OPC).

Where appropriate, in an effort to avoid confusion about phrases like “how much do you trust ‘Organization X’ to protect your privacy...,” the research team used phrases like “how confident are you that ‘Organization X’ will handle your personal information properly and adequately protect it?” By operationalizing ‘trust’ and ‘privacy’ in this way, this research sought to focus on specific issues and minimize the probability of participants misinterpreting the questions.

3.1 FOCUS GROUP INTERVIEWS WITH COMMUNITY GROUPS

The purpose of focus group research is to gather qualitative data about individuals’ beliefs, attitudes and feelings on a topic, with an opportunity to encourage participants to explain their reported views. Selection of the groups (as listed below) was conducted in an effort to involve a general cross-section of the New Zealand population.²⁷

Each participant completed an initial questionnaire consisting of general questions about their trust in the government and concerns about their personal information (see Appendix A). The group interview followed, including a discussion of five general questions and five scenarios (see Appendix B).²⁸ Each question was posed to stimulate discussion related to a specific subject, and to encourage participants to explain what factors influence their views and concerns within the context of this study. Similarly, each scenario was designed to present individuals with a situation involving an improper flow of personal information and asked participants to explain the effect (if any) each scenario would have on them. Several themes and common issues emerged from the various focus group discussions, including people’s differing views about the trustworthiness of government organizations, and individuals’ concerns about current and

²⁶ Due to late cancellations in the first Maori focus group (Group 8i), that group was conducted with only three participants. Therefore, another Maori focus group (Group 8ii) was held and the contributions of both groups are drawn on as one collective group (no participants from Group 8i were involved in Group 8ii).

²⁷ The only requirement for individuals was their willingness to participate.

²⁸ To establish a common understanding of terms, after participants presented and discussed their interpretations of “privacy.” Then, a definition of information privacy was presented to the group to ensure that participants were aware of what was meant by “privacy” for the remainder of the meeting.

future uses of technology (data related to these topics is presented in the Findings section).

While the strength of this focus group research is the richness of information provided, the qualitative data is not necessarily representative of the population, and any inferences should be made with care.

The meetings were conducted from September through November of 2005, and the groups were composed as follows:

- Group 1: Parents (of school-aged children) in a suburb north of Wellington
- Group 2: University students
- Group 3: Recent immigrants
- Group 4: Members of a business association in central Wellington
- Group 5: Parents (of school-aged children) in a suburb of Palmerston North
- Group 6: Members of a suburban business association
- Group 7: Pacific peoples
- Group 8 (i and ii): Maori individuals

3.2 SURVEY OF INDIVIDUALS REPORTING PRIVACY COMPLAINTS

For researchers investigating information privacy, contacting individuals who have submitted a privacy complaint presents a challenge, because that information is confidential and not generally available. As a result of this situation, there is a lack of published research drawing on input from this population. After discussing the objectives of this study with staff members of the Office of the Privacy Commissioner (OPC), that office agreed to help attempt to overcome this obstacle. In order to enable the research team to survey complainants, a protocol carefully designed to protect the privacy of all complainants was followed. In short, after being notified of this research study by the OPC, all respondents were offered an opportunity to “opt-in” in order to participate (as described in Appendix D).

In contrast to the hypothetical nature of focus group discussions, this survey (see Appendix C) collected information from respondents about the consequences of the experience related to their complaint.²⁹ While this survey provides important data about what actually happens when privacy is (believed to be)³⁰ breached, the participants for

²⁹ Instead of questions posed in the form of “how *would* this affect your trust...” this group of participants was asked a series of questions about “how *did* this affect your trust...”

³⁰ The fact that an individual submitted a complaint may imply that they believe their privacy has been breached in some way, but it does not guarantee that this is the case (their complaint may not be well-founded). This is acceptable for this study, as the individual’s belief that their privacy was breached is sufficient.

this survey were self-selecting.³¹ Therefore, any conclusions derived from the results of this survey of complainants are subject to the bias of the sample.

3.3 INTERVIEWS WITH COMMUNITY LEADERS / REPRESENTATIVES

In New Zealand, as in any society, there are groups of individuals that may have a unique perspective regarding their informational privacy (for any number of reasons or personal circumstances, e.g., race, religion, age, health conditions, financial situation, etc.). In designing this study, it was acknowledged that focus groups would provide views from the general population, potentially neglecting the views of those with unique perspectives. Therefore, this study sought the input of individuals believed to have specific knowledge of, or experience with, these groups.³² Individuals fulfilling these requirements were identified by their role within an organization (e.g., the president of an association, or advocates for a specific group of New Zealanders), and contacted by phone or email inviting them to participate in this research. Each semi-structured interview followed a common schedule of questions, which was provided to interviewees well in advance of the interview (see Appendix E).

The main points raised in the interviews are presented in the Findings section. The topics covered were closely related to the themes that emerged from the focus groups, and comparison of the results from each project is included in the Discussion section.

The groups represented in these interviews were:³³

1. Social welfare beneficiaries
2. Ethnic councils in New Zealand
3. Pacific peoples
4. Maori
5. Muslims
6. People with disabilities
7. Women
8. Older New Zealanders (i.e., over sixty years old)

While individuals in the focus groups also presented views from the perspective of these groups, gathering input from these experts and advocates was helpful for corroborating individuals' comments or identifying disagreement within specific groups.

³¹ Each participant in the survey of complainants had submitted a privacy complaint and was required to "opt-in" in order to participate.

³² Based on their experience, interviewees provided more "expert" knowledge than participants in the focus groups and, in nearly every instance, the interviewee was also a part of the group they were representing.

³³ Although several other groups were contacted, some were unable or unwilling to participate.

3.4 SYSTEMATIC ANALYSIS OF QUALITATIVE DATA

Each interview and focus group meeting was recorded and transcribed, providing a large base of detailed data. In order to perform thorough and objective review, the research team used a proven method of coding to analyze this qualitative data. A hierarchical framework of code terms was developed based on the issues discussed in the meetings. Each code term acts as a descriptive label to associate participants' comments with a category and a more specific classification (e.g., if a participant said "I prefer to provide personal information in a face-to-face environment, because I can see how they're treating my information," this comment would be labeled with the code term 'benefit of channel' within the 'Channel' category). The coding framework can be found in Appendix F. This allowed the research team to systematically analyze each transcript and identify comments associated with a specific topic, in turn, facilitating the identification of themes and comparisons among the different groups.

4 Findings

This section reports the data gathered through the three different collection projects (focus groups, survey of complainants, and interviews with community leaders).

4.1 FOCUS GROUPS – QUESTIONNAIRE DATA

Each participant completed an initial questionnaire that collected information about their use of online services, privacy-related concerns and attitudes, as well as their levels of trust in different government organizations.

4.1.1 Background Data

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)³⁴ and/or make purchases from online stores. The resulting statistics are presented in Table 3.

Table 3. Focus group 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

³⁴ See www.trademe.co.nz

These collective statistics allow a rough comparison of the population of focus group participants against similar statistics reported for the national population. Half of all participants reported that they use online banking. Research from late 2003 suggests that 41% of New Zealanders had used online banking as of October 2003 (Taylor Nelson Sofres, 2003). 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. Statistics provided by Trade Me indicate that there are slightly more than one million active members using Trade Me.³⁵ Since this figure includes members who may reside outside of New Zealand (e.g., residents of Australia are permitted to be members), inferences from this number are unlikely to be very reliable.

³⁵ From http://www.trademe.co.nz/structure/media_buyer/site_stats.asp on 8 Dec 2005.

4.1.2 Concerns, Attitudes and Behaviors (prior to discussion)

The initial questionnaire also asked participants to respond to a series of statements about their privacy-related concerns, attitudes and behaviors (using a Likert scale of options, i.e., 1:Strongly agree, 2:Agree, 3:Unsure, 4:Disagree, 5:Strongly disagree). Response data from these questions are shown in Table 4.

Table 4. Reported attitudes, concerns and behaviors

Statement	(n = 58)	SA*	A	N	D	SD	Total Agree (%)	MEAN**
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 <u>private businesses</u> (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 <u>government organizations</u> 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 <u>government organizations</u> "		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 <u>business</u> 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)

** MEAN = Average Response (1 – 5, where 1 represents SA and 5 represents SD)

Thus, the lower the mean score, the more strongly participants tended to agree with the statement.

Many of the topics referred to by these statements were also addressed in the group discussions. For example, responses from S7 and S8 enable a comparison of whether participants have more confidence that their privacy will be protected by government organizations or private businesses, and this question was also raised later in the meetings, when participants were asked to explain their responses. Response data for S6 suggests that a strong 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 to 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) of private businesses before providing their personal information.

Statements receiving a high percentage of neutral responses, like 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 (see Table 4, above) 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). Further comment about the results shown in Table 4 (including how they relate to other data collected in this study) is incorporated into the Discussion section.

The final question (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, as shown in Table 5. These results are interesting, as they indicate that the majority of participants do not assess the trustworthiness of each government organization separately. Later, individuals’ responses to this question during group discussions seemed to contradict this view, as most said that they trust some departments more than others (this will be compared to the findings of other parts of this study in the Discussion section).

Table 5. Levels of trust in different government organizations

Question	Response	#	%
Q16. Do you make distinctions between government departments - do you trust some more than others?			
	Yes (I trust some more than others)	23	41.07
	No (I trust them all the same amount)	33	58.93

Following on from Q16, the questionnaire asked participants to list the government organizations they trust the most, as well as those departments they trust the least.³⁶ While some participants chose not to list any organizations, many others did, and this data is presented in Table 6 and Table 7.

³⁶ Individuals were not prompted with the names of any organizations, so this response data shows only those entities that were nominated by participants.

Table 6. Most trusted government organizations

Organization	Number of Occurrences
Inland Revenue Department (IRD)	6
Ministry of Health (MOH)	4
Work and Income New Zealand (WINZ, within MSD)	3
Department of Labour (DOL)	3
Ministry of Education (MOEd)	2
Immigration (within DOL)	2
Te Puni Kokiri (TPK)	2
Maori Land Court	1
Teachers Registration Council	1
Human Rights Commission (HRC)	1
Department of Internal Affairs (DIA)	1
Electoral Department (within DIA)	1
Birth Deaths and Marriages (within DIA)	1
Studylink (within MSD)	1
Tenancy Services	1

Other responses to this question (most trusted) included: “not any of them,” “they are all the same,” and “none.”

Table 7. Least trusted government organizations

Organization	Number of Occurrences
Inland Revenue Department (IRD)	13
Work and Income New Zealand (WINZ)	13
Ministry of Social Development (MSD)	2
Child, Youth and Family Services (CYFS)	2
Studylink	2
Ministry of Justice (MOJ)	2
Mental Health	2
Ministry of Pacific Island Affairs	1
Department of Building and Housing	1
Ministry of Agriculture and Forestry (MAF)	1
Security Intelligence Service (SIS)	1

Other responses to this question (least trusted) included: “not sure,” “I just don’t trust any of them,” “n/a,” and “they are all the same.”

The data presented in Tables 6 and 7 was gathered prior to group discussions. Later, the same question was also posed in the discussions (asking which departments people trust and allowing participants to explain *why* they trust some organizations and not others, as described later in this section).

4.2 FOCUS GROUPS – DATA FROM DISCUSSIONS

One problematic area of privacy research is the lack of detailed information provided by large-scale, quantitative surveys. Although the results of these surveys may indicate individuals' general level of concern about information privacy, they typically fail to provide reliable information about what influences individuals' concerns and attitudes.

The eight focus group interviews provided a large amount of in-depth data from the various perspectives of the participants involved. After the transcripts were analyzed using the coding framework, the research team was then able to identify the recurring themes and issues raised in the group discussions. 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. Summaries of the findings related to each of the most prevalent topics are presented throughout this section.

4.2.1 Defining Privacy and Gauging Awareness

4.2.1.1 Defining privacy

This study has not sought to develop a new definition of privacy, and this brief discussion of participants' various explanations of the concept is included only to reflect the diversity of their interpretations. To begin each meeting, and introduce the topic of the ensuing discussion, the researchers asked participants to share their view of what the term "privacy" meant to them. In presenting their explanations of what privacy means, many participants mentioned that they believe privacy is related to being able to control "who knows what" about things related with their private lives. Some individuals 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. After listening to the various definitions put forth by individuals, the researchers explained what privacy meant in the context of this study, and presented Westin's definition of information privacy (as cited in the preceding literature review).

4.2.1.2 Awareness of protections

Individuals' privacy concerns may be related to their knowledge about what protections exist to guard their right to privacy.³⁷ 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. Overall, two general patterns of response were observed in the groups. Most commonly, there was quiet uncertainty amongst group members, eventually

³⁷ There are many ways of considering this, for example: if a person does not know that any protections exist, they may be more (or less) concerned about what is likely to happen to the personal information they provide to organizations.

followed by someone mentioning the Privacy Act. At that point, others would acknowledge that they had heard of the Privacy Act, and the majority of individuals reported that they knew little (if anything) about that Act.³⁸ The other response pattern occurred in groups where at least one participant was familiar with Privacy Act based on 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 organizations (the OPC, the Human Rights Commission, etc.) exist to help protect their right to privacy.

Participants expressed various views about their propensity 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. Individuals' 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).

4.2.2 The Trustworthiness of Government Organizations

4.2.2.1 Comparison of trust: Government Vs. non-government organizations

In an effort to learn more about how participants' assess the trustworthiness of government organizations (with specific focus on information privacy), group members 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.³⁹ Overall, the majority of individuals reported having more confidence in government organizations.⁴⁰ One response that was consistent with the attitudes of many participants was:

(From Group 5) *"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, as will be discussed further in section 4.2.2.5.

³⁸ 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.

³⁹ This wording was used to focus on whether participants' trust government or private sector organizations more, within the specific context of their informational privacy (thus, not asking about trust in general).

⁴⁰ 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.

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

(from Group 1) *“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:

(from Group 4) *“I would be more inclined to trust private organizations, ... Government seems to, more and more, want to pry into personal activities.”*

In addition to emphasizing their perceptions about the motivations of these different types of organizations, individuals’ responses seemed to be influenced by their occupation and their general attitude toward public servants (e.g., expectations they expressed about public servants’ competence, motivations and accountability). That is, 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 views supporting government organizations.

4.2.2.2 How trustworthy are different government organizations?

The researchers also asked participants to discuss whether they consider 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.⁴¹

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.⁴²

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 WINZ, among others. Similarly, various comments indicate 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

⁴¹ In these discussions, very few people said that they trust all (or even most) government entities equally (those who trusted all government organizations similar amounts were more likely to report low levels of trust).

⁴² The objective here is not to “name and shame” organizations, but to concentrate on the reasons people gave for trusting or distrusting organizations.

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. One participant recounted a recent interaction he had with Statistics New Zealand, in which he was asked to provide a large amount of information that he considered to be quite personal (as part of a study being conducted). Although he said he had been skeptical at first, he explained that his confidence was sufficiently raised by two things: the collector's thorough explanation of the process (and patient responses to his questions), and the seemingly robust protocol being used to protect his privacy while collecting his information.⁴³

4.2.2.3 Does mistrust propagate through the Government?

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. Very few individuals indicated that it might affect their assessment of the trustworthiness of government organizations in general, while most comments were aligned with the assertion that:

“...it's not so much a government thing, these are government agencies, but I would view each agency as a complete separate entity, and a breach of ethical faith in IRD would make me question IRD and not worry about other institutions.”

Although this response may seem rational (and was commonly articulated in various terms throughout different groups), other statements made during the focus group meetings seemed to contradict this assertion. That is, in discussions where the majority of individuals claimed that a breach of privacy by one government organization would affect only their level of trust in that single entity, some of the same individuals presented generalizations about the trustworthiness of government organizations based on their experiences with one or two specific organizations.

4.2.2.4 Channels: Confidence and concerns

In order to learn more about individuals' concerns and preferences within the context of this study, the research team asked questions about participants' attitudes towards various channels used to interact with government organizations. The researchers were not

⁴³ Given the role and responsibilities of Statistics New Zealand, this may not be surprising. Other large government departments likely have fundamentally different relationships with citizens and may face different challenges.

specifically interested in which channel people believe to be the most convenient or usable. Instead, the focus was on which channel people consider more trustworthy for providing personal information, and the initial question was presented as: “When you need to provide personal information to a government organization, which channel do you have the most confidence in – that your privacy will be protected?” The responses within and among the various groups reflected a diverse range of opinions and justifications for the views presented.

Face-to-Face

The overwhelming majority of people reported that they have the most confidence when they provide their personal information in a face-to-face environment (this was consistent across all groups). Individuals provided a variety of explanations for their consistent support of this channel, including:

- the ability to interact with and have a relationship with the person receiving their information,
- the ability to see how the recipient is receiving and treating their information,
- the ability to judge the competence of the individual receiving the information,
- the ability to check the accuracy of the information submitted, and
- the belief that they can hold someone accountable if something goes wrong.

Post

The next most preferred channel for providing personal information was the post. Participants provided a number of reasons for having confidence in this method, including:

- familiarity with filling in paper forms (comfort based on previous experience),
- the ability to review the information upon completion,
- the ability to make copies and retain a record of the information they submit, and
- a high level of understanding around what happens with forms they post (in contrast to submitting information online).

A number of group members also voiced certain disadvantages to sending information via post, including:

- inadequate knowledge of who is receiving the information (and how they are treating it);
- the possibility that mail can be lost or intercepted;
- and concern about how the information is processed once it arrives at its destination (including worries that information may be entered inaccurately into computer systems).

The Internet

Participants' confidence related to submitting information via the Internet resulted in the greatest diversity of views about the various channels available. In many groups, this channel was slightly preferred to the telephone, but people generally reported less confidence compared to face-to-face and the post. During the discussions, people often distinguished between "secure" websites⁴⁴ and websites in general, with significantly higher levels of confidence in secure websites. 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.⁴⁵ 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.

Phone

Individuals consistently reported low levels of trust in providing personal information by phone. Reasons provided for these attitudes included:

- no tangible record of the event,
- difficulty authenticating the individual on the other end of the conversation;
- inability to see how the information is being treated, and
- foreign accents of some operators (it was suggested that this causes some uncertainty about where information is going)

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.

Does the channel matter?

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.

⁴⁴ In explaining what they meant by secure sites, individuals often related this to the presence of a padlock displayed along the browser window, or a message notifying them that they were entering a secure website. Some participants (in different groups) reported that they have confidence in websites advertising that they have been "proven secure."

⁴⁵ Comments related to concerns about the Internet and other technologies are shown in Tables 9 – 11.

4.2.2.5 Data Sharing

Not surprisingly, most groups raised the issue of data sharing between government organizations during various parts of the discussions. Individuals' comments on this subject showed distinct contrast between the attitudes of participants. A number of individuals reported that they believe data sharing programs are fundamentally breaches of information privacy,⁴⁶ while others claimed that government data sharing programs contributed to a feeling of having little control over where their personal information is communicated (e.g., from Group 2 "I don't think you have too much control with the government, and different government departments, because they just share information").

On the other hand, many people expressed qualified support for certain sharing arrangements, including some who were quite positive about the potential for data sharing. These supporters noted 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 information multiple times to different government organizations and said that they would rather have the information shared between certain entities. Comments suggested that this type of sharing would be acceptable in situations where, for instance, an individual has provided their information to IRD and then is also required to provide that information to 'Organization X,' some would rather just authorize Organization X to get their information from IRD.⁴⁷ The divergent views are illustrated in the comments below, from two members (A and B) of the same group.

(From Group 5)

A : "...the conspiracy theory I have that they, that [government organizations] all share information stops me, makes me think twice before I tell them the truth. It's not that I lie to them, but I'll give them my name and address and let them figure it out."

In response, another group member (B) expresses their contrasting view:

B: "Well, I prefer sometimes for them to share, I get sick of going through all the same information again... well can you not check it out with IRD, they've got it all there ... and I just find that quite annoying"

The most commonly cited benefit of data sharing was convenience (e.g., avoiding the hassle of re-submitting the same information to different organizations), and no participant mentioned 'saving tax dollars' as a perceived benefit.

⁴⁶ These fundamental objections were most commonly based on the logic of: 'if I provide my information to one organization and they share it with another organization, that is wrong and unacceptable.'

⁴⁷ This example is included to clarify that participants expressed greater support for having the ability to authorize data sharing on a case-by-case basis, rather than data sharing operations that do not require their informed consent.

4.2.3 Prevailing Themes and Recurring Topics

4.2.3.1 Power distribution in the state - citizen relationship

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.

Table 8. Comments: The power of government organizations

Group	Quotation
1	[talking about large, central government departments] "... <i>with those sorts of organizations, you don't feel very empowered, to say 'No I am not giving [my personal information] to you'</i> "
2	[talking about government organizations in general] " <i>like you have more control over what [information] you give to the private business over like the government ... you can't really say to them I can't give you that, I can't tell you that because they sort of, ... I have the idea that the government can find it out if they want to.</i> "
5	[talking about government organizations in general] " <i>we've seen it right through the years they can fob it off...you can't really do anything against government</i> "
8	[talking about personal experience with WINZ] " <i>No, they have this power thing over you, ... it's like, you know, (speaker slams fist on table) [they're] the boss.</i> "

Table 8 provides examples of related comments made in different groups. Since information privacy relates to an individual's ability to determine who their personal information is communicated to and what it is used for, this commonly asserted belief (that individuals have minimal power and control in this relationship), may be particularly influential in shaping citizens' attitudes in this context.

4.2.3.2 Technology: Concern and lack of understanding

As shown in the preceding literature review, many issues related to information privacy are inextricably linked to technology. Participants' comments commonly included concerns and observations about how different technologies seem to pose risks to their information privacy.

Due to the diversity of participants in the focus groups, comments reflected many different levels of knowledge about computers, the Internet, and technology in general (from inexperienced and uneducated / untrained, to experienced and educated / trained). Throughout the groups, most of these issues and concerns were raised in relation to individuals' personal experiences and stories they had heard through various media channels. Comments about technology generally involved one or more of three themes: concerns about the security of computers and the Internet, worries related to 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.

The most frequently mentioned group of concerns was focused on security issues related to computers and the Internet. Participants consistently reported anxiety about the trustworthiness of the Internet as a medium for communicating personal information; often expressing fears about "hackers" and various stories they had heard (see Table 9).

Table 9. Comments: General security and privacy concerns related to the Internet

Group	Quotation
1	[talking about sending personal information over the Internet] <i>"With the Internet, I'm always really worried about who else can, not the organization, but which hacker's going to get my information"</i>
2	[explaining concerns about the Internet] <i>"I think just because it's so open, and it's, you know, it's really hard to determine what is secure and what isn't secure..."</i>
8ii	[explaining attitude towards the Internet] <i>"I don't trust [the Internet] at all, too many cyber people out there."</i>
5	[explaining why he does not trust the Internet for communicating personal information] <i>"people say, 'yeah, the internet's quite safe,' but the hacker's job is to bypass any new information, you know, and it's a constant, as soon as they've pulled out one product, ...they've got something they can bypass it with, and within forty-eight hours they reckon, from the time something new comes out, you can get around it. Yeah, so not much faith in the internet myself."</i>
6	[responding to question about whether any stories in the media influence concerns] <i>"What one reads ... definitely one reads that emails are open to severe abuse"</i>

In addition to worries about the security of information communicated via the Internet, individuals expressed concerns about the security of computers and databases that can be compromised via the Internet or otherwise (see Table 10). Some comments about this issue included assertions that people feel there is more potential for significant breaches of information privacy based on the increasing use of information technology.

Table 10. Comments: Concerns about the insecurity of personal information

Group	Quotation
1	[expressing concern about the insecurity of personal information on computers] <i>"It annoys me more that <u>people can actually lift the information and it doesn't matter how... confidential it supposedly is, people still gain your name, they gain your address, they hack in, they get your email, they get whatever.</u>"</i>
4	[expressing concern about the insecurity of personal information on computers] <i>"[Hackers] got into the Pentagon, I mean, do I think that they could get into my doctor's records or the IRD, if they can get into the Pentagon, (sarcastically) ... It's just possible that my GP doesn't have as many protections as the Pentagon."</i>
7	[expressing concerns related to technology and personal information] <i>"This new technology has <u>banished all notion of privacy.</u> As people have <u>easy access to private information that needs to be kept secured.</u>"</i>
5	[expressing doubt about organizations' ability to secure personal information] <i>"If a hacker wants to get in, they'll get into the servers, I mean, all those big companies have remote server access for people working, people managing them, so [hackers] have a way of getting into them"</i>
4	[about personal information being in digital form on computers] <i>"it's now <u>computerized and much more likely to be seen.</u> I think it's a very hazardous, very dangerous situation." ... "Well, <u>once you've got things sitting on a database somewhere then, then any number of people</u> who wanted to get in and have a look at it, can get in and have a look at it"</i>
7	[expressing fear about the availability of information and potential for damage] <i>"Looking at modern technology, and how privacy has resulted in an increase of lawlessness, and <u>people finding ways to access personal information...</u> so there's <u>always that fear, that one day they will have access to disclose it.</u>"</i>

Although levels of fear were higher in those individuals who reported having less experience using the Internet, experienced Internet users⁴⁸ also voiced concerns and distrust, including the comments shown in Table 11.

⁴⁸ Including individuals educated in information technology and trained to work with computers.

Table 11. Comments: Concerns from experienced and educated users

Group	Quotation
2	[talking about sending personal information over the Internet] <i>“I studied [information technology] for a while so I don’t have much confidence in the security [of the Internet]”</i>
8ii	[explaining why he does not trust the Internet for communicating personal information] <i>“For me, just because, for myself, because I work with computers ... people that are quite brainy these days, they can, ..., attach something to your email and it extracts your information and you wouldn’t know, or they make a program for your bank account details through a café,... it’s probably the worst [channel] for me”</i>

Another type of technology-related concern was based on participants’ feeling of having insufficient knowledge about the Internet and information technology in general. Individuals reported that, although government organizations gave them assurances about the protections in place to keep their information confidential, individuals had very little knowledge about how (or whether) this was achieved, and some doubted whether they would be informed if something went wrong. A number of comments comparing the Internet to other channels suggested that this lack of understanding caused individuals to be less confident in the Internet, for instance:

“I don’t really understand the Internet, I don’t understand it all, but I can understand, you write on a piece of paper, [or] you go and talk to someone, because that’s something you know, you’re well aware of.”

Based on a number of the comments made in different groups, some individuals believe that it is common for hackers to intercept their communications, or intrude into computer systems to steal their information. For example, as individuals complained about unsolicited contact through postal mail and telephone calls, an individual implied that the postal address and phone number were likely gained by hacking when she asserted: “So they’ve hacked in somewhere to get that info on you.”⁴⁹

4.2.3.3 Organizational Situation Handling

Throughout discussions about the scenarios presented and the personal experiences participants shared with each group, the researchers posed questions about how (or whether) certain events would impact on individuals’ level of trust in the organizations involved. As they explained the effect each scenario would have, two factors commonly raised by participants were: 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.

⁴⁹ Although this information *could* have been gained through hacking, it is seemingly more likely to have been gained through more traditional means of information brokering (e.g., the sale of customer lists).

Punishment for wrongdoing related to personal information

In many groups, participants emphasized the importance of the actions an organization takes to punish employees who breach privacy. When the researchers asked questions about whether specific scenarios (each involving a different type of improper information flow) would have an effect on participants' trust in an organization, numerous individuals reported that the effect could be minimized as long as they knew the organization adequately punished the responsible individuals. This concept was raised in relation to a number of very different scenarios (minor breaches and major breaches), for example: after discussing a case where employees of a large government department were discovered violating citizens' privacy for personal financial gain, the researchers asked whether this would have any impact on participants' trust in that organization. While many reported that this would have an adverse effect on their trust in the organization, others reported that, as long as the individuals were punished appropriately, this would not have an impact on their trust (see Table 12).

Table 12. Comments: The influence of punishment

Group	Quotation
5	[response to a question about whether a breach of privacy would affect one's level of trust in a government organization] <i>"Well that's the thing, you're trusting the government, because they are doing that, <u>they're finding the people</u> that are doing it, and <u>they're found and punished</u>. ... And they're pulling these people out and getting rid of them."</i>
8i	[response to instance where employee deliberately breaches a citizen's privacy] <i>"<u>I trust them more</u> if there was a <u>heavy penalty</u>, like I knew they'd be dumped for [that breach]"</i>
1	[response to a case where government employees sold citizen's information] <i>"As long as there's penalties for anyone doing that sort of thing, that's severe enough to put most people [off]... that the government takes these things seriously"</i>

This concept was also evidenced by participants' personal anecdotes. After one researcher asked about why individuals trust some departments more than others, one person shared the following:

"I have to say I really trust in IRD, because I know of an instance where somebody was working at Inland Revenue, checked up his daughter's [personal information] and was fired on the spot. So I know they... take their privacy literally" (this person heard this story from a friend)

Organizational honesty

In cases where privacy is breached, the importance of the way the offending organization treats the individual (victim), was expressed through discussions comparing different scenarios. Opinions presented in different groups emphasized the importance of an organization being honest, candid and sincere towards the individual. When organizations met these conditions, many individuals claimed that this would reduce (or even nullify) any negative impact on their trust in the organization.

For example, given a scenario where an organization notified a participant that her sensitive personal information was accidentally mailed to the wrong address, the researchers asked whether the incident would affect her level of trust in the organization:

“Not if they’re honest, if they rung and said it was in [error], because I mean, everyone makes mistakes, but if they just owned up and said ‘We made a mistake,’ ..., then I wouldn’t be bothered really”

For more significant breaches, this factor was reported as having less power to mitigate a decrease of trust.

4.2.3.4 Consequences of a breach

In each group, participants explained how various scenarios had affected, or would affect, the amount of trust they place in different organizations.⁵⁰ The overwhelming majority of individuals reported that breaches of information privacy have an impact on their trust in organizations (i.e., breaches affect their assessment of the trustworthiness of the organization). These responses suggest that a number of variables seem to influence the magnitude of the impact on individuals’ trust. These factors include:

What was the perceived cause of the breach? In increasing order of adverse consequences, people distinguished between general categories of: an honest mistake, staff incompetence, deliberate wrongdoing, and/or motivated by financial gain.

How sensitive was the information involved? Not surprisingly, the more sensitive the information, the greater the impact a breach would have. Individuals generally reported that health information and financial information are the most sensitive (in that order), while a few individuals claimed that their contact details were the most sensitive (these individuals explained that they did not want previous acquaintances to be able to find them).

What happened to the information? If the information was improperly disclosed, the magnitude of the impact was influenced by the entities it was disclosed to (i.e., Who received the information?).

How did the organization handle the situation? Individuals emphasized the importance of an organization’s response to any privacy-related situations, as was addressed in the previous section (i.e., How did they treat the individual? Was the organization perceived to be up-front and honest? What is the organization doing to ensure this will not occur again?, etc.).

⁵⁰ This included their reactions to previous personal experiences, as well as their responses to the hypothetical scenarios presented by the researchers.

Has this type of event happened before / is this event consistent with, or contradictory to, the organization's reputation? When explaining how much an event would impact their level of trust, individuals commonly said this would depend on whether the problem was perceived to be a "once-off" or not. Individuals were more likely to "give the organization the benefit of the doubt" in cases where an event appeared to be a unique aberration from an otherwise trustworthy reputation.

Also, although some people reported being relatively unconcerned about their privacy, many others became quite emotional as they recounted personal experiences. In one group, an individual repeatedly slammed her fist on the table as she explained an instance where she believed WINZ had shown disregard for her privacy. She then apologized, "Sorry, I'm getting all hyped up." In another group, after listening to others sharing negative experiences with IRD, a man stated with frustration, "*talking about all of this makes me really angry because I just had a bad experience with these people [employees of IRD].*" This type of emotional response was most often shown by individuals who reported having an unfavorable first-hand experience with a government department.

4.2.3.5 Participants' reported attitude Vs. behavior

Another noteworthy issue relates to the fact 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. An illustration of this comes from a discussion where individuals were talking about their concerns about using the Internet as a channel for providing personal information. One particular individual in the group repeatedly insisted that he had no trust in the Internet and wouldn't ever send personal information over the Internet. This individual reported that he worked with computers in his job, claiming that he consistently observed "*things going wrong*" with computers and the Internet, and affirmed "*I'd never trust [the Internet] for personal information.*" As a follow-up question to this comment, a researcher asked whether he used online banking or Trade Me for online transactions. After a long pause, the individual smiled and admitted that he used both services on a regular basis (online banking and Trade Me). This participant explained that, although he did not trust the Internet, the convenience of being able to do things online was sufficient motivation for using these services. 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.

4.3 SURVEY OF COMPLAINANTS TO THE OPC

The purpose of the survey of individuals who had made a complaint to the OPC was to learn about the consequences of privacy breaches from individuals who believed that their privacy had been violated. More specifically, the survey was designed to collect information about how respondents' attitudes and behaviors changed after the incident related to the privacy complaint they filed. In addition to their level of trust in the specific organization (which they believe breached their privacy), if an individual reported having filed a complaint against a government organization, information was gathered on their level of trust in government organizations in general. Data was also collected about individuals' willingness to provide personal information to organizations before and after the alleged breach, along with information about changes in their behavior.

One hundred and ten complainants were notified of this study and were offered an opportunity to participate in this research. As outlined in the Methodology section, after being notified of this study, each complainant had to contact the research team in order to request a survey, and twenty-four individuals did this. Seventeen completed surveys were returned from participants geographically distributed throughout New Zealand. Although the total number of surveys completed was lower than anticipated, each survey provided detailed information about the respondent's attitude before and after the incident related to the complaint they filed.

4.3.1 Reported Level of Trust: Before and After

Table 13 presents response data for questions five and six (Q5 and Q6), which enable comparisons between participants' reported level of trust in the specific organization that they believe breached their privacy (before and after the event). 76.5 percent of respondents reported a decrease in trust towards the organization after the incident.⁵¹ While 58.8 percent of all respondents reported having "very **trusting**" or "moderately **trusting**" attitudes towards the organization *prior* to the event (Q5), 82.4 percent reported that their attitude towards the organization *after* the event was "very **untrusting**" (Q6).

Table 13. Trust in organizations, before and after incident

Question	(n = 17)	VT*	MT	U	MU	VU	MEAN**
Q5. "Before the incident related to the complaint I filed, my attitude towards <u>the specific organization</u> that I feel breached my privacy was:"		4	6	3	2	2	2.53
Q6. "After the incident related to the complaint I filed, my attitude towards <u>the specific organization</u> that I feel breached my privacy was:"		1	0	1	1	14	4.59
Q8. "Before the incident related to the complaint I filed, my attitude towards <u>government organizations in general</u> was:"		2	9	1	3	0	2.33
Q10. "After the incident related to the complaint I filed, my attitude towards <u>government organizations in general</u> was:"		0	0	0	4	11	4.73

* Abbreviations: VT = "Very trusting" MT = "Moderately trusting" U = "Unsure"
 MU = "Moderately untrusting" VU = "Very untrusting"

** MEAN = Average Response (1 – 5, where 1 represents VT and 5 represents VU)

⁵¹ Where an individual's affirmed attitude after the event (Q6) was less trusting than before (Q5).

88.2 percent of respondents reported that the organization they believed breached their privacy was a government organization. One section of questions (Q8 - Q12) was answered exclusively by this group,⁵² in order to collect data about how an individual's experience with one government organization affects their attitude, including their attitude towards government organizations in general. This group of participants completed Q8 and Q10, which asked about their level of trust in government organizations in general, before and after the incident (see Table 13). 86.7 percent of this group claimed that their level of trust in government organizations in general had decreased from before the incident to after it.⁵³

All those participants who claimed a government organization had breached their privacy reported having either a "moderately untrusting" or "very untrusting" attitude toward all government organizations in general, after the event, including 73.3 percent reporting "very untrusting" attitudes for after the incident (see Q10). This result may contradict the responses given by many focus group participants, who reported that if one organization breached their privacy, this would only affect their level of trust in that organization and would not have an impact on their level of trust in all government organizations.

4.3.2 Willingness to Provide Personal Information

Questions 11, 12, 15 and 16 asked each respondent about their willingness to provide personal information to organizations (again, at both specific and general levels), and response data for these questions is provided in Table 14, below. All participants answered Q15 and Q16. 82.4 percent of respondents reported that they were less willing to provide personal information to the **specific** organization that had breached their privacy (answering either "Strongly agree" or "Agree" for Q15, including 64.7 percent who agreed strongly). 82.4 percent also reported that they were less willing to provide personal information to **any** organization after the event (see Q16 in Table 14). While the overall percentages of individuals agreeing with the statements in Q15 and Q16 were equal, the data shows that the magnitude of this agreement was distributed differently, with more participants reporting stronger prejudices against the specific organization involved.

⁵² For Q8 through Q12, n = 15.

⁵³ Where an individual's reported attitude after the event (Q10) was less trusting than before (Q8).

Table 14. Willingness to provide information, attitudes and behavior

Question	(n = 17)	SA*	A	U	D	SD	MEAN**	Total Agree (%)
Q11. “After the incident related to the complaint I filed, I am less willing to provide my personal information to <u>any government organization</u> , regardless of whether they have mishandled my personal information.”		5	7	2	1	0	1.93	80.0
Q12. “As a result of the incident related to the complaint I filed, I have refused to provide personal information to a <u>government organization</u> (once or multiple times) because I don’t trust them with my information.”		1	7	1	3	0	2.50	53.3
Q15. “After the incident related to the complaint I filed, I am less willing to provide my personal information to <u>the specific organization</u> that I feel breached my privacy.”		11	3	0	2	0	1.56	82.4
Q16. “After the incident related to the complaint I filed, I am less willing to provide my personal information to <u>anyone</u> (government organizations, private organizations, etc.).”		5	9	1	1	0	1.88	82.4

* Abbreviations: SA = “Strongly Agree” A = “Agree” U = “Unsure” D = “Disagree”
SD = “Strongly Disagree” Total Agree = (Strongly Agree + Agree)

** MEAN = Average Response (1 – 5, where 1 represents SA and 5 represents SD)

Thus, the lower the mean score, the more strongly participants tended to agree with the statement.

Q11 and Q12 were answered only by respondents who had filed privacy complaints against government organizations. 80 percent of this group affirmed that they were less willing to provide personal information to **any government organization**, regardless of whether the organization had mishandled their information (answering either “Strongly Agree” or “Agree” for Q11). Q12 asked participants about whether they had behaved in a distrusting way, and 53.3 percent reported that, as a result of the incident, they had refused to provide personal information to at least one government organization. Two other participants did not select an answer for this question, and instead commented that the opportunity to refuse to provide personal information to a government organization had not yet arisen.

4.4 INTERVIEWS WITH COMMUNITY LEADERS / REPRESENTATIVES

The purpose of interviewing representatives and advocates was to collect information that would supplement the data gathered through the focus groups and the survey of complainants. Each participant received the interview questions (see Appendix E) prior to meeting with the researcher, and in order to help validate their responses, most reported that they had sought input from other members of the group they were representing. This section presents the main points raised in each interview.

4.4.1 Interview #1: Social welfare beneficiaries

Several beneficiary advocates (including some who had been beneficiaries themselves) were interviewed as a group.⁵⁴ Most of this discussion was primarily focused on beneficiaries' interactions with Work and Income New Zealand (WINZ). Interviewees emphasized that the relationship between beneficiaries and WINZ is characterized by an imbalance of power and control, and that beneficiaries generally have had low levels of trust in government. Another factor said to influence this group's attitudes towards (and levels of trust in) the government involved the perception that some government publicity campaigns have been seen as characterizing beneficiaries as "fraudsters" and criminals. The participants also explained that, based on their experiences, many social welfare beneficiaries are not highly educated and know very little about what laws or protections existed to protect their rights.

Interviewees reported that beneficiaries tend to believe that they have very little control over what information they provided to WINZ and other government agencies, and suggested that the quantity and type of information this group provided to the government makes them particularly vulnerable to having their sensitive information mishandled. Also, the issue of government data sharing and matching programs was raised as a cause of considerable fear and anxiety amongst beneficiaries.

Interviewees provided several examples of situations where beneficiaries information had been mishandled by WINZ employees,⁵⁵ and mentioned multiple stories in the media that had influenced this group's concerns: "*We generally get a flurry of comments from clients [beneficiaries]... after publicity about a privacy breach.*" In addition to providing anecdotes involving breaches of information privacy, interviewees expressed frustration that, most often, attempts at recourse were ineffective because "*you can't really track it back through the system... to prove that the information was wrongly given out.*" In response to a question about whether stories involving privacy breaches have an adverse effect on individuals' confidence, an interviewee said, "*I think it impacts greatly on concerns, one negative story is worth a lot,*" and another added "*Because [as a result] you can't give assurances*" that people's information will be handled properly.

⁵⁴ This format was used because the group felt (collectively) more able to represent the attitudes and experiences of social welfare beneficiaries.

⁵⁵ e.g., one interviewee reported that, because of an error made by WINZ, he had recently received sensitive personal information about hundreds of local beneficiaries (which he had no right to receive).

4.4.2 Interview #2: Ethnic councils in New Zealand

A representative of various ethnic councils in New Zealand raised a number of issues from this group's perspective. The participant explained that, since a high percentage of members of ethnic groups (or their parents) have immigrated to New Zealand, their attitudes towards the government are often significantly influenced by their attitudes towards (and experiences dealing with) the government of the country they have come from.⁵⁶ Along similar lines, the interviewee explained that historical events can have significant, long-lasting effects on people's attitudes towards government and, therefore, this group's level of trust in government varies greatly. This individual also noted that, although members of this group tended to be intelligent and skilled, they were likely to have less knowledge about laws and human rights in New Zealand.

The representative mentioned that people generally seemed to have more confidence in government organizations (compared to others), and this was partially due to the perception of transparency and accountability, because any governmental wrong-doing would likely be made public and result in negative publicity. However, the interviewee also said that the recent increase in data sharing among government organizations was a source of concern about the future, noting that people seemed especially concerned about the potential for linkages between types of information and anxiety about moving towards a 'Big Brother' government. Similar to other groups, the representative noted that individuals' concerns appear to be strongly influenced by media reports about stories involving breaches of privacy and confidentiality.

4.4.3 Interview #3: Pacific peoples

To complement the input collected from the focus group of Pacific peoples, an individual representative was also interviewed. This individual suggested that Pacific peoples have generally had low levels of trust in the government, largely based on historical events and stories communicated about personal experiences. The interviewee emphasized the effect that the "dawn raids" (controversial efforts to detain illegal immigrants, which occurred during the 1970s and involved multiple government organizations) have had on Pacific people's attitudes towards the New Zealand Government. Specifically related to the issue of information privacy, the individual stated that these events have resulted in "*a lot of mistrust about what information is held, who accesses that information, and a lot of fear as well.*"⁵⁷ Later in the interview, the participant commented that most of this group's mistrust towards government is likely related to their attitudes towards large departments like Work and Income New Zealand, Inland Revenue, the Department of Child, Youth and Family Services, and the Immigration Service.

⁵⁶e.g., if an individual comes from a country where the government is highly corrupt and abusive of its citizens, this likely influences their attitudes towards the New Zealand Government.

⁵⁷ The interviewee also explained that high percentages of predominately Pacific communities (around Porirua) refused to complete the most recent census, suggesting that this may have been a manifestation of attitudes of mistrust about how the information would be used.

The representative also explained relevant aspects of cultural issues in Pacific communities, including the importance of keeping family matters private, and protecting the reputation of one's family name. The participant suggested that this group's "concerns about their personal information and how it's handled is often driven by what they know about how it should be handled or don't know about it, and more than not, they don't know much." Another issue thought to be unique to (or more pronounced in) Pacific communities is that individuals "very rarely complain" via any complaints process. Instead of complaining to the organization (or other relevant entities), they are much more likely to tell others in the community about their negative experiences, which does not help organizations to address their concerns or their dissatisfaction. The interviewee also affirmed that there is concern about what information is being shared between government agencies, and that this is related to people's confidence that their privacy would be respected. Moreover, she suggested that many Pacific people have a low level of understanding about what they are agreeing to when they complete forms for government organizations, and how the information is used:

"The issue is that they don't really understand what they're filling out, and because so many of them are dependant on government, I would say that... they do care how their information is managed, but I don't think they have that much trust with government because of their lack of understanding of how – who's sharing information."

In regard to this group's attitude towards technology, the interviewee stated that many Pacific people in New Zealand do not have access to computers and the Internet, which contributes to a lack of experience and familiarity with these technologies. The individual also noted that those people who were born in New Zealand (in comparison to recent immigrants) are more likely to be comfortable using computers and online services (based on having more experience with, and exposure to, these technologies).

4.4.4 Interview #4: Maori

To complement the information collected in the Maori focus groups, two representatives of Maori were interviewed (their occupations and experiences made these individuals particularly suited to participate in this study, and the age difference between them helped to provide input from two different generations).

The interviewees expressed the view that Maori have generally had low levels of trust in the New Zealand Government. In addition to the underlying mistrust resulting from controversy over issues related to the Treaty of Waitangi, other more recent issues were also mentioned as sources of mistrust (including the "Foreshore and Seabed" disputes that led to the 2004 Hiko (march), and the way various politicians had recently supported proposals to eliminate government programs designed to help Maori). The two individuals suggested that Maori tend to have different attitudes towards various parts of the government, trusting some more than others. While many Maori may tend to have more trust in organizations that are believed to help Maori communities (e.g., the

Ministry of Maori Development (TPK), the Maori Language Commission and the Maori Broadcasting Commission), they said that many Maori (often in lower socio-economic classes) tend to distrust the Police and other government organizations.

Presenting Maori perspectives and concerns about information privacy, interviewees discussed several aspects of Maori culture. The participants noted that, although sharing personal information is seen as an important part of Maori culture, this is typically done orally and there are sensitive issues related to recording Whakapapa (Maori genealogy) and other personal information. These issues include concerns about identity theft and losing control over personal information.⁵⁸ One interviewee also commented that some government organizations have been insufficiently sensitive to Maori cultural issues when collecting personal information.⁵⁹ Interviewees also suggested that there is not a high level of understanding amongst Maori about which organizations are parts of the government and which are not.

The representatives suggested that media stories have had a significant influence on Maori attitudes towards the government and concerns about the privacy of their personal information. For some Maori, they explained that events like the “dawn raids” of the 1970s still fuel a sense of mistrust towards the government, while more recent cases seem to have a greater impact on current levels of trust. For example, they cited widely publicized allegations in 2003-04 about a New Zealand Security Intelligence Service (SIS) operation (referred to as “Operation Leaf”) allegedly designed to spy on Maori organizations and individuals. Regardless of whether the allegations surrounding Operation Leaf were accurate, the coverage of the story was said to have caused significant concern amongst Maori, and seems to influence their attitudes towards the government.

In response to questions about Maori attitudes towards using technology and the Internet to interact with government, interviewees discussed potential obstacles including insufficient access to resources and low levels of computer literacy. Although they indicated that Maori prefer to interact in a face-to-face environment, it was also suggested that younger Maori would be increasingly likely to interact using the Internet, as the younger participant (age 20 – 29) commented, “*for my generation, we’re more comfortable [using technology and the Internet] because it’s the way we communicate with people.*”

⁵⁸ An interviewee explained that, since so much of one’s identity and entitlements are based on one’s ancestry and personal details, some Maori believe that sharing of recorded personal information has potential for negative consequences.

⁵⁹ e.g., In handling issues like ‘Whangai’ – or Maori adoption, where issues of legal parenthood are different from traditional Pakeha (European) adoption. While government guidelines may exist in relation to handling Maori adoption, it was suggested that some organizations do not consistently follow these guidelines.

4.4.5 Interview #5: Muslims

Two representatives of Muslims in New Zealand were interviewed. These individuals explained that a high percentage of this group have immigrated to New Zealand, often coming from third world countries. As a result, they suggested that individuals' attitudes towards the government are largely influenced by the cultural and emotional "baggage" they have brought with them. Based on the participants' experiences, many individuals in this group are generally less concerned about privacy issues and more focused on meeting "lower-level" needs. Furthermore, it was suggested that the concept of privacy carried different connotations for Muslims, explaining that the term is often more closely associated with private family information (which tend to be very sensitive), rather than other personal details.

One interviewee explained that he had recently noticed changes in the attitudes and behaviors of many Muslims, saying "*as of late... many Muslims seem to be not forthcoming with information... when it comes to the public arena, they'd rather be non-descript and anonymous.*" The other individual corroborated this view of recent changes in attitudes and behaviors, and they both voiced significant concerns about the "new laws," in reference to new counter-terrorism and terrorist financing legislation. Although they were not very familiar with the particular details of the legislation, they believed it could allow the government to subjectively declare that an organization or individual had supported terrorists (e.g., based on donations made to organizations that may later be declared to be linked to terrorism). The interviewees suggested that uncertainty, and concern about what consequences these new laws might have, are a cause of worry amongst many Muslims in New Zealand.

4.4.6 Interview #6: People with disabilities

An individual representing the unique perspective of people with disabilities was interviewed. Speaking about this group's general level of trust in the government, the representative explained that most people with disabilities tend to trust some government organizations more than others. It was suggested that this is based on individuals' personal experiences and what people know (or have heard) about each organization. As an illustration, the interviewee noted that the Ministry of Health's Disability Services Directorate (DSD) is generally more trusted than many of the health screening programs that the Ministry of Health was responsible for. The representative explained that the DSD has earned the trust of disabled people, "*gradually, through successive iterations of our concerns – there's a general belief that we'll be listened to.*" In contrast, she said that individuals' previous experiences with health screening programs have called into question the trustworthiness of the organizations responsible for ensuring that the information is handled properly, and has resulted in significant mistrust (specifically about how the information will be used, and who will have access to it).⁶⁰

⁶⁰ The interviewee cited the Gisborne Cervical Cancer Screening Inquiry as an example of a case where individuals' personal information was mishandled, having an adverse affect on individuals' trust and confidence.

The representative emphasized the importance of protecting the privacy of personal health information, as breaches in this area seem to make people less willing to share important information with medical practitioners, *“We don’t want some person going into our records to see [the information we provide], we can’t trust them [to keep this confidential], so we won’t say.”* The interviewee also suggested that organizations and workers tend to be less respectful about disabled individuals’ right to privacy, *“if you’re disabled, it seems that all your details become anyone’s property.”*

The interviewee said that another serious concern relates to the “information gap” between individuals with disabilities and those who collect and use their information, *“without knowing what happens to your information – you can’t even begin to address the privacy concerns if you don’t know what you need to know. Informed consent is important.”*

Another issue that was raised included concerns about the National Health Index (NHI). The participant suggested that there was uncertainty about what information will be associated with the NHI in the future, and what the information will be used for. Related to data sharing, the participant suggested that sharing of information among government organizations was a “serious worry” to this group, and this contributes to a feeling of vulnerability and having inadequate control over where one’s information is communicated.

4.4.7 Interview #7: Women

Although ‘women in New Zealand’ is a very general classification, it was suggested that women have a sufficiently unique perspective, and the interviewee representing this group raised a number of relevant points. Similar to other interview participants, in addition to having extensive experience and relevant knowledge, the individual sought input on the interview questions from many other women before meeting with the researcher.

The participant explained that many women reported that their trust in the government was decreasing, largely because of the increasing reliance on information and communications technologies (ICT), *“it’s not necessarily that they don’t trust the government – it’s that they don’t trust the technology”* involved in the operation of government.⁶¹ The individual also reported that women claimed to have various levels of trust in different government organizations, and that most made distinctions between the trustworthiness of politicians and public servants. However, she said, *“there’s a lot of blurring of boundaries,”* explaining that there is some confusion about which organizations are part of the government and which are not.

⁶¹ e.g., *“Yes, they’re concerned that if the government goes to entirely electronic collection, it will become more easy for ‘hackers and spammers and scammers’ whatever else you want to call them, to get into that information somehow.”*

The interviewee suggested that women tend to have more confidence that their privacy will be protected by government organizations compared to other organizations. This, she explained, is related to their worries about the increasing frequency of identity theft and the general belief that the private sector is more involved in activities that lead to identity theft. Also, although many women are aware of the Privacy Act and the Official Information Act, she said “*they don’t know the content of those acts,*” and “*there’s a lot of misinformation*” about the provisions of the Privacy Act.

Specifically talking about women’s views related to informational privacy, the interviewee provided examples of instances where women’s personal information has been misused⁶² and suggested that these occurrences are causes of serious concerns. The participant affirmed, “*those issues are influencing people’s trust in government systems,*” and clarified, “*there is an issue of concern about how the information [collected by government organizations] **might** be used,... what might [the government] do with [the information]?*” These concerns, she suggested, have been minimized by some organizations that clearly explain why certain information is being collected and how the information will be used (e.g., Statistics New Zealand). The interviewee also reported that a number of women she had talked with said they were unwilling to provide any personal information that did not seem specifically necessary for a given interaction.⁶³

On the topic of data sharing, the representative suggested that, while most women seem to be reasonably accepting of data sharing programs, they are concerned about how government organizations ensure that sharing and matching is done accurately and fairly.

4.4.8 Interview #8: Older New Zealanders

The perspective of older New Zealanders was provided through an interview with a representative of an organization that performs advocacy for this group. The participant suggested that older New Zealanders generally have a moderate level of trust in the government and, within ‘the government,’ most individuals tend to differentiate between the trustworthiness of politicians and public servants.

In relation to their concerns about privacy and providing personal information to government organizations, the representative suggested that older New Zealanders tend to be uncomfortable when organizations request seemingly irrelevant information from them. He advised that members of this group often become frustrated if government employees do not satisfactorily explain why the requested information is needed, and he said this contributes to a view that government employees are saying “*‘you’ve got to give [your information], so give it’ rather than, ‘we need this information because, for these reasons.’*” The individual affirmed that, when government organizations fail to explain

⁶² The participant cited a number of health screening programs for women where privacy was allegedly breached.

⁶³ e.g., “*A lot of them say ‘If a form says we want your date of birth,’ they refuse to fill in the form, unless there’s a very solid reason for the need of date of birth.*”

why requested information is needed, *“that leads to a loss of trust and confidence that information is relevant and isn’t simply being taken for the sake of being collected.”*

The interviewee also asserted that many older New Zealanders have concerns about the sharing of data among government organizations, and clarified that these concerns seem to be fueled by a lack of knowledge about data sharing programs (which organizations are sharing information, what information is being shared, what is the purpose, etc.). Furthermore, he explained, their concerns seem to be strongly influenced by stories in the media about government organizations mishandling citizens’ personal information, suggesting: *“that destroys the confidence that they have in [government organizations’] ability to handle material confidentially.”*

In relation to older New Zealanders’ use of technology, the participant noted that many individuals in this group are not computer literate, and are generally uncomfortable using computers.⁶⁴ He commented that many individuals have concerns about “hackers” and the confidentiality of information communicated via the Internet, and these anxieties would likely be obstacles to their use of the Internet, *“that’s the same reason that older New Zealanders will just totally resist Internet banking and all those sorts of things, because of the perceived concerns that they have about privacy and access and hackers.”*

⁶⁴ He also noted that computer literacy campaigns are helping some older New Zealanders gain experience using computers and the Internet, but many have little or no experience.

5 Discussion

In order to address the questions presented at the outset of this report, this research study collected information from a diverse range of New Zealanders. While the data sets and findings from each of the three projects (focus groups, survey of complainants, and interviews) are valuable independently, the comparisons that they collectively enable provide richer and more complex data than any single project. Many of the findings have been presented in the preceding section and need not be restated here. Instead, this discussion ties together the associated results from these separate projects, and relates their implications to the research questions that motivated this study.

Listening to the views expressed by those who participated in this research, we have repeatedly been reminded about the unique challenges 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). The diversity of reported perspectives is a reflection of the different attitudes, beliefs, feelings and experiences of the citizens served by the New Zealand Government. This range of views is also a positive indication that participants felt comfortable to voice their opinions and did not feel obligated to reach consensus on issues. While diversity makes generalizations more challenging, the findings have provided many insights related to the various areas we set out to explore.

5.1 CONCERNS ABOUT INFORMATION PRIVACY

One of our primary interests has been to learn about the concerns New Zealanders have about the privacy of their information. The findings of the focus groups and the interviews illustrate the various concerns expressed by the groups represented. Two main categories of concerns raised were: technology-related concerns, and concerns specifically related to government organizations. After listing some of the major concerns within these categories, the factors that individuals suggested were most influential in shaping these concerns will be discussed.

Concerns linked to technology can be divided into two sub-categories: general concerns, and concerns specifically associated with communicating information via the Internet. Participants reported that these issues were often causes of fear and considerable anxiety, and those who expressed fear were more likely to have less experience with technology and the Internet.

1. Concerns associated with technology included:
 - General technology-related concerns:
 - Belief that the widespread use of computers, databases, and the Internet have increased the potential for damaging privacy breaches

- Lack of understanding about how information technology works, resulting in uncertainty and/or fear about how personal information is collected, processed, stored, etc.
- Belief that “hackers can get any information they want” from databases, including government databases.
- Belief that individuals have little control over what happens to their information
- As a combination of the above, fear that “our increasing reliance on computers and technology” will continue to reduce individual privacy
- Concerns about communicating personal information via the Internet:
 - Uncertainty about what happens to information submitted online (in contrast to a more familiar process, like posting a letter)
 - Belief that information submitted online may not be confidential and can be intercepted by “hackers”
 - Fear based on inexperience and lack of understanding, “I’m scared of the Internet because I don’t understand it”

Participants most commonly reported that their technology-related concerns were driven by information from media sources and seldom based on their own experiences or the experiences of people close to them. The other main driver for these anxieties was a general lack of understanding about issues related to information technology and the Internet. This combination of factors, widely publicized stories about Internet-related threats and system vulnerabilities (e.g., hackers, crackers, viruses, insecurity of operating systems, etc.), along with insufficient knowledge about these issues, seem to promote widespread concerns. However, while most individuals reported that these anxieties greatly reduce their confidence, they would not necessarily prevent them from using computers and the Internet. Media stories were also said to fuel people’s worries about identity theft and a sense that their personal information is increasingly available to others. The significant influence of media content on individuals’ privacy-related concerns supports the assertions of other research (Raab & Bennett, 1998).

Before discussing the common types of government-related privacy concerns, it is important to note that some participants acknowledged that using technology could potentially result in enhanced individual privacy. For example, some people may be uncomfortable discussing sensitive issues (e.g., finances, relationships, health conditions, etc.) with others, including public servants. 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.

2. Concerns specifically related to government organizations involved:
 - Belief that individuals have little control over what information they provide to the government (e.g., “What choice do I have? I have to give them the information they ask for.”)

- Belief that individuals have little control over how government organizations use their personal information, including worries about their information being used for additional purposes without their informed consent
- Uncertainty about whether employees are properly trained and competent
- Uncertainty about government data sharing: how it is conducted, what information is involved, and what protections are in place to protect information privacy. Concerns about data sharing influence other concerns (e.g., lack of control over information)

In contrast to concerns about technology, concerns about the trustworthiness of government organizations were more often reported to be the result of personal experiences (as evidenced by several personal anecdotes) and domestic cases where parts of the New Zealand Government were believed to have breached individuals' privacy (e.g., the "dawn raids," government employees prosecuted for selling citizens' personal information, rumors about "Operation Leaf" allegedly designed to spy on Maori groups and individuals, mismanagement of medical information collected for health screening programs, etc.). As shown in the above list, these concerns reflect a distinct perception that individuals have little control over the personal information they provide to government organizations, and generally lack power in their relationships with these organizations.

While personal experiences with government organizations were more influential, media stories about the government were also reported to affect individuals' concerns and confidence. Many participants referred to programs they had watched on television⁶⁵ and attention-grabbing headlines that appear regularly in printed sources (e.g., "Government scheme fuels privacy concerns" (Bell 2004, April 26)). Although it is difficult to judge whether the content presented through media channels reflects healthy skepticism or cynical mistrust, information from these sources certainly affect individuals' attitudes.

5.2 AWARENESS OF PRIVACY PROTECTIONS / REGULATIONS

It is not surprising that the findings suggest the majority of individuals had very little knowledge about the Privacy Act of 1993 or any regulations that exist to protect their information privacy. On this matter, interviewees representing the various groups (who often suggested that individuals were unlikely to know about rules governing their information privacy), corroborated the views expressed in the focus group meetings. Despite their reported concerns, individuals' comments suggested that they were not sufficiently interested to learn about the provisions of the Privacy Act, and those who

⁶⁵ The consumer program "Fair Go" was the most frequently mentioned television show, often with reference to stories about identity theft or other misuses of personal information.

were aware of the Act commonly reported that their familiarity was due to their occupation. The findings also indicate that some individuals question the effectiveness of the available forms of recourse, contending that once privacy-related harm is done, this often cannot be rectified (in contrast to losses that are strictly financial).

5.3 HOW TRUSTWORTHY ARE GOVERNMENT ORGANIZATIONS?

The vast majority of focus group participants and interviewees indicated that individuals assess the trustworthiness of each government organization separately, and therefore, they trust some more than others. However, many comments made during focus group discussions suggested that people do make generalizations about the expectations they have for government organizations in general (e.g., “Oh that’s just a typical government department stuff-up”). This tendency to generalize is also supported by the data collected from focus group participants prior to group discussions, as reported in Table 5, where the majority reported that they trust all government organizations the same amount.

Findings from the focus groups and the interviews suggest that the majority of individuals consider government organizations to be more trustworthy than private organizations, with regard to information privacy, which supports the general findings of Cullen and Hernon (2004). While various justifications for this view were provided, most were related to people reporting greater confidence in the motivations and objectives of government. Other comments in support of government bodies frequently included perceptions about the greater transparency and accountability of these organizations, in comparison to private businesses. However, many participants expressed uncertainty about whether public servants in various organizations are properly trained and competent.

While individuals voiced some uncertainty about data sharing (including some who were strongly opposed to it), many people voiced qualified support for these programs. Participants most often reported that their concerns about the interchange of data between government organizations were related to their lack of knowledge about what data sharing involves and that this contributed to feelings of having their information passed around outside of their control. In addition to further corroborating the results of Cullen and Hernon (2004), these findings are consistent with those of “Privacy and Data-Sharing: Survey of public awareness and perceptions,”⁶⁶ which identified “lack of control” over personal information and “lack of knowledge [about] what is being done with it” as key sources of concerns about government data sharing (2003).

The findings also indicate that some people believe privacy breaches that occur in the private sector are more likely to pass without media coverage, thus private businesses do

⁶⁶ This report was based on a survey of individuals in Great Britain and Northern Ireland.

not have such a strong disincentive (negative media attention) compared to government agencies.

5.4 WHAT HAPPENS TO TRUST WHEN PRIVACY IS VIOLATED?

The results of the data collected through the survey of complainants and the focus groups suggest that breaches of privacy often have an adverse effect on individuals' trust in the offending organization. While this may seem intuitive, the focus group findings show that many people reported that certain breaches of privacy would not affect their trust at all, depending on the circumstances and the way the situation was handled by the organization.

The survey findings also show that a high percentage of respondents was less willing to provide personal information to organizations (to the specific organization, as well as to any other organizations) after the incident. While these attitudinal measures are noteworthy, it may be more interesting that the majority of respondents that complained against government organizations reported that they had actually refused to provide their personal information to a government organization as a result of the breach they perceived. While these results may be influenced by the bias of the sample, they provide interesting insight into the attitudes of individuals before and after a breach and indicate potentially important areas for future research.

In order to minimize the negative consequences of privacy breaches that occur, it may be useful to consider the factors that participants reported were the most influential. Members of focus groups indicated that the following variables were the most important dimensions for predicting the effect that a breach of privacy would have on their trust:

- What was the perceived cause of the breach? (e.g., honest mistake, incompetence, deliberate wrongdoing, etc.)
- How sensitive was the information involved? (i.e., to the specific individual, since different types of information had varying levels of sensitivity)
- What happened to the information? (e.g., if disclosed, who was the information disclosed to?)
- How did the organization handle the situation? (i.e., Was the organization honest and sincere, and did it take action to ensure the situation would not occur again, including punishment for those responsible?)
- Has this type of event happened before? (i.e., Was the event consistent with, or contradictory to, the organization's reputation?)

The explanations provided by participants should help to identify why some breaches have a greater impact than others. The fact that participants said it was important that an organization punish those who are responsible for a breach of privacy was not unexpected, as Fox et al. (2000) also found that individuals were supportive of punishing

wrongdoers responsible for privacy breaches. However, it was not expected that this “punishment” variable would affect individuals’ trust as significantly as it was shown to.

5.5 DO THE CONSEQUENCES OF A BREACH PROPAGATE?

This issue was raised in the focus groups as well as through the questions in the survey of complainants. Some of the associated findings from these two projects appear to contradict each other, which may be related to the different populations involved. Focus group participants repeatedly affirmed that if one government organization breached their privacy (regardless of the degree of the breach), this would only affect their trust in that organization (e.g., “it’s not fair to blame all of the government, no matter how much I would like to”). In contrast, the results of the survey of complainants support the idea that when one government organization is perceived to breach an individual’s privacy, this not only erodes their trust in the specific offending organization, but is likely to have an adverse effect on their level of trust in other government organizations as well. As Table 13 shows, the decrease in participants’ trust toward the offending organization was more pronounced than this generalized reduction of trust.

Among many possible reasons for this discrepancy, this may relate to the seriousness of the breach, as well as the personal and emotional dimensions of incidents related to individual privacy. Some individuals will not complain when they feel their privacy has been violated, and it seems reasonable to expect that those individuals who submit privacy-related complaints to the OPC are dissatisfied enough to seek redress through that process. It is also unlikely that hypothetical scenarios capture any emotional aspect of an incident as effectively as personal experiences. Although the explanations provided by focus group participants sounded rational and reasonable, they may not have been realistic forecasts of the actual effect a breach would have on their attitudes. Since very little research has been conducted on this important area, further investigation is needed to draw more concrete, reliable conclusions about the consequences that privacy breaches have on individuals’ trust.

5.6 CONFIDENCE IN CHANNELS:

Based on findings from the focus groups and interviews, individuals consistently reported having the most confidence in providing personal information in a face-to-face environment. While the post was also regarded highly, there was widespread skepticism about privacy online, and individuals expressed the least confidence in providing information by phone.

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 that the most New Zealanders have security concerns about (Curtis et al., 2004).

The most important positive characteristics of a channel (for providing personal information) were:

- Interaction with a person (some form of relationship)
- Ability to retain a record of the event
- Ability to check the accuracy of information being submitted
- Ability to understand how one's information is delivered to the destination point

5.6.1 Confidence in the Internet

Individuals' assessments of the trustworthiness of the Internet were extremely varied, including some reporting moderate levels of confidence and others who have no trust in it at all. Nearly all focus group participants and interviewees expressed concerns about the privacy of information submitted online (via websites and email). Despite their concerns, half of all focus group participants reported that they use online banking and many also use Trade Me and/or make purchases from e-commerce websites. Numerous people who said that they had fears about doing things online explained that those fears did not prevent them from using online services, implying that they were willing to accept risks in exchange for the benefits that they perceived. The most commonly reported benefit of doing things online was convenience, which is consistent with the findings of Curtis, et al. (2004).⁶⁷ These patterns also support the conclusions of Fox et al., who found that despite individuals' reported anxieties, people "behave in surprisingly trusting ways in many sensitive online areas" (2000, 12). It is also probable that the majority of individuals may be unaware of the risks associated with online activities, which would hinder their ability to accurately assess these risks when making decisions.

⁶⁷ This quantitative research found that the two most commonly reported reasons for using the Internet over other channels were the convenience and speed of doing things online (Curtis et al. 2005, 8).

F. Conclusion

The New Zealand E-Government Strategy is aimed at improving the integration and efficiency of government information and services, and has the long term goal of “transforming” government⁶⁸ through the use of information and communications technologies (ICTs). While there are significant potential benefits associated with using ICTs to improve government performance, performance is not the only objective of government. In order to promote and maintain citizens’ trust, government organizations must find ways to build relationships with people within the relatively new environment of e-government. This report has shown that there is not a high level of concern among New Zealand citizens about the way government agencies collect and store their personal information. In this context, around 60 percent of participants expressed confidence (see Table 4), and only between 15 and 21 percent express distrust, or lack of confidence in how their personal information is handled by government agencies. However, there are issues raised in this report that government should take notice of. These issues focus on anxieties expressed by citizens across a range of social groups, and center around two key factors affecting citizens’ perceptions about how well their personal information is managed: the increasing use of technology in collecting, processing and storing personal information; and the relationship between citizens and government. These factors impact considerably on the degree of trust that citizens are willing to place in government organizations in relation to their personal information, and must be addressed if trust is to be maintained and enhanced.

There are a number of issues that government organizations need to consider in relation to the issue of trust and privacy in the e-government environment. Firstly, citizens show limited understanding about what happens to information communicated via the Internet, what their rights are in relation to personal privacy, and how data sharing between government agencies is regulated in New Zealand. Risks associated with online transactions are not well understood, and although many people currently seem willing to accept these risks, people feel vulnerable and uncertain about communicating personal information via the Internet. In New Zealand, individuals have the right to be informed about how their personal information is collected and used by government organizations and government websites. The New Zealand Government Web Guidelines⁶⁹ are now mandatory for government websites and require websites to include statements about privacy and security. Often these statements are not prominently displayed, nor widely read by users. Although statements attempt to be user friendly, they routinely do not define technical terms such as ‘cookies,’ and do not offer any assurances about the security of data held. If citizens are unable to easily access and understand these privacy statements or policies, the potential value of this requirement will not be realized. In addition, the privacy statements on most government websites relate to the use made of names/addresses or IP addresses, and the use of cookies to gather information about site visitors, and those requesting further information from the site. Most organizations do not

⁶⁸ E-government vision, mission, goals and outcomes <http://www.e.govt.nz/about-egovt/strategy/strategy-june-2003/>

⁶⁹ The Guidelines are mandatory as of January 2006, retrieved from <http://www.e.govt.nz/standards/web-guidelines/web-guidelines-v-2-1/> 6 January 2006.

include any statement about data submitted by individuals for official purposes, or provide links to the Privacy Commissioner's web site, where the privacy principles are set out. General privacy principles, enshrined in New Zealand law, need to be more widely promulgated on New Zealand government websites.

The second major area where government organizations could go further towards meeting the concerns of citizens expressed in this report, is in taking a more proactive approach to the building of relationships between government and citizens in the online environment. Citizens' perceptions about the trustworthiness of government organizations are related to what they know about those organizations, especially based on their own personal experiences. If the Internet is to play the major role foreshadowed in the goals of the E-Government Strategy,⁷⁰ then ways of enabling citizens to build a relationship with an agency through its web site will be increasingly important. This must be part of the transformation of government envisaged in the E-Government Strategy, which focuses on citizens as well as government agencies. Moving interactions to the online environment changes the nature of citizens' dealings with government, and may de-personalize relationships, which can make trust more difficult to establish and retain. In order to successfully engender citizens' trust, government organizations need to adopt an appropriate communications model for promoting their relationships with individuals. This may involve increasing individuals' ability to customize and personalize government websites to foster a sense of belongingness in users. Given that citizens believe most breaches of privacy are caused by incompetence of staff (rather than malicious action) and poor information security practices, it is essential to establish sound codes of practice for organizational employees, as well as appropriate departmental policies and training to promote trustworthy behavior and respect for privacy. While these actions may be pre-conditions for building trust, these measures will not necessarily bring about this result on their own. However, with the right principles in operation and protections in place, information privacy (and citizens' perceptions of information privacy) can be enhanced rather than diminished, given that the Internet allows for the exchange of information without the citizens having to hand their information to an intermediary, or engage in face-to-face encounters.

This project has barely scraped the surface of these issues. Far more research is needed to determine what communication models will be most effective in the context of e-government, and which of these models will encourage citizens' to consider shifting their interactions with government to the web, rather than relying on face-to-face

⁷⁰ Two major goals of this strategy are:

“By June 2007, networks and Internet technologies will be integral to the delivery of government information, services and processes.

By June 2010, the operation of government will have been transformed through its use of the Internet.”
(E-government vision, mission, goals and outcomes <http://www.e.govt.nz/about-egovt/strategy/strategy-june-2003/>)

communication and postal services because of trust issues. This communication model must achieve a difficult balance - it must empower citizens in their relationship with government, while at the same time acknowledging the power imbalance that operates between government and citizens, an imbalance that the majority of participants in this study were acutely aware of. Like the balance between personal privacy and public interest, examined by many scholars in this field (Westin 1967, Etzioni 1999), a balance between the powerful role of the state and the ideal of the greater empowerment of the citizen through e-government must be attempted. If these critical balances can be achieved, then the vision of making the Internet the primary means for citizens to communicate with government may itself be achieved. If "information supplied by citizens to government is the indispensable handmaiden of the modern activist state" (BeVier, 1995), then it must be respected and used in ways that enhance democracy and the rights of citizens and not diminish them.

REFERENCES

- Barnes, C. & Gill, D. (2000). "Declining Government Performance? Why Citizens Don't Trust Government." Working Paper, New Zealand State Services Commission. Retrieved 12 October 2005, from <http://www.ssc.govt.nz/display/document.asp?docid=2891>
- Bellman, S., Johnson, E.J., Kobrin, S.J., & Lohse, G.L. (2004). "International differences in information privacy concerns: a global survey of consumers." *The Information Society*, 20, 313-324.
- Bennett, C. J. & Raab, C. D. (2003). *The Governance of Privacy: Policy instruments in global perspective*. Hampshire, England: Ashgate.
- BeVier, L.R. (1995). "Information About Individuals in the Hands of Government: Some reflections on mechanisms for privacy protection." *William and Mary Bill of Rights Journal*, 4, 455-506.
- Booz Allen Hamilton. (2005). *Beyond e-Government: The world's most successful technology-enabled transformations*. 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
- Consumer Reports WebWatch. (2005). *Leap of Faith: Using the Internet despite the dangers*. Retrieved 12 November 2005, from <http://www.consumerwebwatch.org/view-article.cfm?id=10720&at=510>
- Council for Excellence in Government. (2003). *The New E-Government Equation: Ease, engagement, privacy and protection*. Retrieved 30 September 2005, from <http://www.excelgov.org/usermedia/images/uploads/PDFs/egovpoll2003.pdf>
- Council for Excellence in Government. (2004). *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>
- Cullen, R. & Hernon, P. (2004). *Wired For Well-Being: Citizens' Response to E-Government*. Report to the E-Government Unit of the State Services Commission. Retrieved 2 December 2005, from <http://www.e.govt.nz/resources/research/vuw-report-200406>
- Curtis, C., Vowels, J., & Curtis, B. (2004). *Channel-Surfing: How New Zealanders Access Government*. Auckland UniServices. Retrieved 5 December 2005, from <http://www.e.govt.nz/resources/research/channel-surfing-200409>

- Dempsey, J.X., Anderson, P., & Schwartz, A. (2003). "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. Retrieved 5 May 2005, from <http://www.internetpolicy.net/privacy/20030523cdt.pdf>
- Dinev, T. & Hart, P. (2004). "Internet Privacy Concerns and Their Antecedents – Measurement validity and a regression model." *Behaviour and Information Technology*, 23 (6), 413 – 422.
- Dinev, T., Belloto, M., Hart, P., Colautti, C., Russo, V., & Serra, I. (2005). "Internet Users' Privacy Concerns and Attitudes towards Government Surveillance – An exploratory Study of Cross-Cultural Differences between Italy and the United States." *18th Bled eConference: eIntegration in Action*. Bled, Slovenia.
- Electronic Privacy Information Center and Privacy International. (2004). *Privacy and Human Rights 2004: An international survey of privacy laws and developments*. Retrieved 14 October 2005, from www.privacyinternational.org/survey/
- Electronic Privacy Information Center. (2005). "Public Opinion on Privacy." Retrieved 2 August 2005, from <http://www.epic.org/privacy/survey/default.html>
- Etzioni, A. (1999). *The Limits of Privacy*. New York: Basic Books.
- Fox, S., Rainie, L., Horrigan, J., Lenhart, A., Spooner, T., & Carter, C. (2000). "Trust and privacy online: Why Americans want to rewrite the rules." Pew Internet & American Life Project, Washington, DC.
- Friedman, B., Kahn, P. H. Jr, & Howe, D. C. (2000) "Trust Online." *Association for Computing Machinery. Communications of the ACM*, 43(12), 34 – 40.
- Fukuyama, F. (1996, Dec 2). "Trust still counts in a virtual world." *Forbes*, 33-34.
- Gandy, O. H. Jr. (2003). "Public Opinion Surveys and the Formation of Privacy Policy" *Journal of Social Issues*, 59(2), 283 – 299.
- Hardin, R. (2002). *Trust and Trustworthiness*. New York: Russell Sage Foundation.
- Hu, Q. & Dinev, T. (2005). "Is Spyware an Internet Nuisance or Public Menace." *Communications of the ACM*, 48(8), 61-66.
- Kent, S. T. & Millett, L. I. (2003). *Who Goes There? Authentication Through the Lens of Privacy*. Washington, DC: National Academy Press.

Kerber, M. & Thomas, A.M. (2003). "The Erosion of Privacy After September 11: A call to arms for the protection of the attorney-client relationship in the face of a national crisis." *The Georgetown Journal of Legal Ethics*, 16(4), 693.

Klosek, J. (2000). *Data Privacy in the Information Age*. Westport, Connecticut: Quorum Books.

Koppe, K. (2002). "Data Protection and the Internet – A comparison of the approaches towards data protection in the European Union, the United States and New Zealand." Victoria University of Wellington.

Liu, C., Marchewka, J.T., Lu, J., & Yu, C.S. (2005). "Beyond Concern—a privacy-trust-behavioral intention model of electronic commerce." *Information & Management*, 42, 289–304.

Market and Opinion Research International. (2003). "Privacy and Data-Sharing: Survey of public awareness and perceptions." Retrieved 21 June 2005, from <http://www.dca.gov.uk/majrep/rights/mori-survey.pdf>

Milberg, S.J., Burke, S.J., Smith, H.J., & Kallman, E.A. (1995). "Values, Personal Information Privacy, and Regulatory Approaches." *Association for Computing Machinery. Communications of the ACM*, 38(12), 65.

Milberg, S.J., Smith, H.J., & Burke S.J. (2000). "Information Privacy: Corporate management and national regulation." *Organization Science*, 11(1), 35 – 57.

Moore, B. Jr. (1984). *Privacy – Studies in Social and Cultural History*. Armonk, New York: M. E. Sharpe.

Nelson, L. (2004). "Privacy and Technology: Reconsidering a crucial public policy debate in the post-September 11 era." *Public Administration Review*, 64(3), 259.

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

Olivero, N. & Lunt, P. (2004). "Privacy Versus Willingness to Disclose in E-commerce Exchanges: The effect of risk awareness on the relative role of trust and control." *Journal of Economic Psychology*, 25, 243–262.

O'Neill, O. (2002). *A Question of Trust*. Cambridge: Cambridge University Press.

Organization for Economic Cooperation and Development [OECD]. (1980). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. OECD, Paris. Retrieved 2 August 2005, from http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

Prebble, M. (1990). *Information, Privacy, and the Welfare State: An integrated approach to the administration of redistribution*. Wellington: Victoria University of Wellington, Institute of Policy Studies.

Prosser, W.L. (1960), "Privacy." *California Law Review*, 48, 383-89.

Raab, C.D. & Bennett, C.J. (1998). "The Distribution of Privacy Risks: Who Needs Protection?" *The Information Society*, 14, 263 – 274.

Raab, C.D. (2004). "The future of privacy protection." UK Office of Science and Technology, Retrieved 8 August 2005, from http://www.foresight.gov.uk/Previous_Projects/Cyber_Trust_and_Crime_Prevention/Reports_and_Publications/the_future_of_privacy_protection.pdf

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

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). "Not So Different After All: A cross-discipline view of trust." *Academy of Management. The Academy of Management Review*, 23(3), 393–404.

Smith, H.J., Milberg, S.J., & Burke, S.J. (1996). "Information Privacy: Measuring individuals' concerns about organizational practices." *MIS Quarterly*, 20(2), 167.

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

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

Spiekermann, S., Grossklags, & J., Berendt B. (2001). "Stated Privacy Preferences Versus Actual Behaviour in EC environments: a reality check." *Proceedings of the 5th International Conference Wirtschaftsinformatik (Business Informatics) - Finanzdienstleistungen (Information Systems in Finance) WI-IF 2001*, German Informatics Society, Augsburg, Germany. 129-148.

State Services Commission. (1998). *Personal Information Protection and Public Confidence: Confidentiality and security of citizens' personal information held by the Inland Revenue Department and Work & Income New Zealand*. Report by the New Zealand State Services Commissioner. December 1998.

Swartz, N. (2003). "Information at a price: Liberty vs. security." *Information Management Journal*, 37(3), 14.

Taylor, S. Jr. (2003). "Rights, Liberties, and Security." *The Brookings Review*, 21(1), 25.

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

United Nations. (1948). *Universal Declaration of Human Rights*. Retrieved 10 September 2005, from <http://www.un.org/Overview/rights.html>

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

United States Department of Health, Education and Welfare [HEW]. (1973). *Code of Fair Information Practices*. Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens viii.

Warren, S.D. & Brandeis, L.D. (1890). "The Right to Privacy." *Harvard Law Review*, 4(5), 193-220.

Westin, A. (1967). *Privacy and Freedom*. New York: Atheneum.

APPENDIX A: Focus Group Questionnaire

Initial questionnaire

Please answer the following questions, ticking the check boxes that best represent your situation:

Q 1. Gender: Male Female

Q 2. Age: (Please tick the one that describes you)

- 15-19 20-24 25-29 30-34 35-39
 40-44 45-49 50-54 55-59 60-64
 65-69 70+

Q 3. Occupation:

Q 4. Do you use the Internet for e-mail or searching the web?

- Yes No

Q 5. Do you use online banking, Trade-me or purchase from online stores?
(please tick all that you use)

- Online banking Trade-me Online stores (e.g. Amazon)

Q 6. I am concerned about the privacy of my personal information when it is exchanged online via the Internet.

- Strongly agree Agree Neutral Disagree Strongly disagree

Q 7. 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.

- Strongly agree Agree Neutral Disagree Strongly disagree

Q 8. I feel confident that my personal information will be handled properly and adequately protected by the government organizations I deal with

- Strongly agree Agree Neutral Disagree Strongly disagree

Q 9. I trust government employees to treat my personal information with appropriate respect for my privacy.

- Strongly agree Agree Neutral Disagree Strongly disagree

Q 10. I am generally concerned about the amount of information that various government organizations hold about me.

Strongly agree Agree Neutral Disagree Strongly disagree

Q 11. I usually seek or check statements about the way in which my personal information will be protected before I supply information to government organizations.

Strongly agree Agree Neutral Disagree Strongly disagree

Q 12. 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.

Strongly agree Agree Neutral Disagree Strongly disagree

Q 13. I think the rules governing the way in which government organizations collect and exchange information about me are adequate.

Strongly agree Agree Neutral Disagree Strongly disagree

Q 14. 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.

Strongly agree Agree Neutral Disagree Strongly disagree

Q 15. When I need to provide personal information to government, I feel most confident that the privacy of my personal information will be best protected when I communicate (please rank 1 – 4, where “1” is for the channel you have the most confidence in and “4”, the least):

- by phone
- in Person
- on the Internet/by Email
- via Post

Q 16. Do you make distinctions between government departments - do you trust some more than others?

Yes (I trust some more than others) No (I trust them all the same amount)

Which departments do you trust the most?

Which departments do you trust least:

APPENDIX B: Focus Group Scenarios⁷¹

1. A letter from the Ministry of Social Development about your household income supplementary benefit gets sent to another beneficiary in error, and you are notified by MSD after the other person calls them to tell them about receiving your letter.
2. You are leaving your Council office where you have called in to pay your rates, when you see papers lying around, clearly dropped by some Council officer. As you pick them up to hand them to a clerk, you realize that they refer to a dispute between someone you know, and the Council over unpaid rates on a property whose ownership is under dispute. It all looks very acrimonious (but highly intriguing) and you are slightly shocked by your neighbor's intemperate language.
3. You are visiting a close neighbor in hospital, and call in at the nurses' station to ask about whether you can make arrangements to take her home the following day, since she has no relatives in the city. As you lean across the desk you realize that you can see her health record up on a screen, with some fairly personal information there about her psychological state. It looks to you as though just about anyone passing by could see this information if they wanted, certainly anyone working in the hospital, and perhaps casual visitors like yourself.
4. You change your address via NZ Post's Change of Address website (www.changemyaddress.co.nz), and when you are offered 8 entities that you can notify of your move, you tick the box for 5 of the 8. You later find out, via receiving mail or otherwise, that two of the three that you didn't tick found out about your new address from the info you submitted through the NZ Post site, and you are now being bothered with unwanted emails from a political party.
5. A recent prosecution of a staff member employed at Inland Revenue for selling tax information about individuals to debt recovery firms shocked many people, and raised questions about the checks on staff in government agencies from breaching trust in this way. . . How distressing is this? (Explain the details to participants and encourage them to discuss their attitudes / reactions)

⁷¹ These basic scenarios were presented and explained in order to begin discussions.

APPENDIX C: Survey of Complainants

Note about questions 1 and 2: Remember, we do not know anything about your privacy-related case. However, since I am investigating a variety of aspects of privacy in relation to cases like yours, I would be grateful if you would tell me two general things about your case by answering **Q1** and **Q2**.

Q1. The alleged privacy breach in my case was related to:

- 1.) Denying me access to information about myself
- 2.) Improper disclosure of information about me
- 3.) Inaccurate information about me
- 4.) Other (please specify) _____

Q2. In my case, the entity that I felt breached my privacy was:

- 1.) My employer
- 2.) Not my employer

Background

Q3. When I deal with government organizations, I feel **most** confident that my privacy will be protected if I provide personal information:

[Please rank the choices 1 to 4: (1) for the most confidence and (4) for the least confidence]

- ___ In a face-to-face environment (e.g., speaking with a representative in an office)
- ___ By mail
- ___ Using the Internet
- ___ Using the telephone

Q4. I believe that the breach of my privacy came about because of:

- 1.) An honest mistake
- 2.) Disregard for my privacy (inadequate training of staff, improper processes, etc.)
- 3.) Malicious snooping into my affairs
- 4.) Other (please specify) _____

Trust and the Organization that breaches privacy

Q5. Before the incident related to the complaint I filed, my attitude towards the specific organization that I feel breached my privacy was:

1.)Very trusting 2.)Moderately trusting 3.)Unsure 4.)Moderately untrusting 5.)Very untrusting

Q6. After the incident related to the complaint I filed, my attitude towards the specific organization that I feel breached my privacy was:

1.)Very trusting 2.)Moderately trusting 3.)Unsure 4.)Moderately untrusting 5.)Very untrusting

Q7. In my case, the entity that I felt breached my privacy was:

- 1.) A government organization (e.g., ministry, department, council, tertiary institution, hospital, etc.)
- 2.) Not a government organization (e.g., bank, store, credit reporting firm, etc.) - Please skip to **Q13**

Government organizations and trust

Q8. Before the incident related to the complaint I filed, my attitude towards government organizations in general was:

1.)Very trusting 2.)Moderately trusting 3.)Unsure 4.)Moderately untrusting 5.)Very untrusting

Q9. Before the incident related to the complaint I filed, when I provided my personal information to government organizations I felt confident that my personal information would be handled properly and adequately protected.

1.) Agree strongly 2.) Agree 3.) Unsure 4.) Disagree 5.) Disagree strongly

Q10. After the incident related to the complaint I filed, my attitude towards government organizations in general was:

1.)Very trusting 2.)Moderately trusting 3.)Unsure 4.)Moderately untrusting 5.)Very untrusting

Q11. After the incident related to the complaint I filed, I am **less** willing to provide my personal information to any government organization, regardless of whether they have mishandled my personal information.

1.) Agree strongly 2.) Agree 3.) Unsure 4.) Disagree 5.) Disagree strongly

Q12. As a result of the incident related to the complaint I filed, I **have refused** to provide personal information to a government organization (once or multiple times) because I don't trust them with my information.

1.) Agree strongly 2.) Agree 3.) Unsure 4.) Disagree 5.) Disagree strongly

---- Please skip to **Q15** ----

Private Organizations and trust

Q13. Before the incident related to the complaint I filed, when I provided my personal information to private organizations I felt confident that my personal information would be handled properly and adequately protected.

1.) Agree strongly 2.) Agree 3.) Unsure 4.) Disagree 5.) Disagree strongly

Q14. As a result of the incident related to the complaint I filed, I **have refused** to provide personal information to a private organization (once or multiple times) because I don't trust them with my information.

1.) Agree strongly 2.) Agree 3.) Unsure 4.) Disagree 5.) Disagree strongly

Willingness to provide personal information after a breach of privacy

Q15. After the incident related to the complaint I filed, I am **less** willing to provide my personal information to the specific organization that I feel breached my privacy.

1.) Agree strongly 2.) Agree 3.) Unsure 4.) Disagree 5.) Disagree strongly

Q16. After the incident related to the complaint I filed, I am **less** willing to provide my personal information to anyone (government organizations, private organizations, etc.).

1.) Agree strongly 2.) Agree 3.) Unsure 4.) Disagree 5.) Disagree strongly

Use of online services

Q17. Before the incident related to the privacy complaint you filed, did you: use online banking, buy goods from online stores, or use TradeMe?

- 1.) Yes (please circle those you used) online banking online stores TradeMe
- 2.) No (if No, please skip to **Q20**)

Q18. Of the choices you selected in **Q17**, please circle those that you still use after the incident:

- online banking online stores TradeMe

Q19. If you've stopped using either online banking, online stores, or TradeMe, is this related to your concerns about: (please circle all those that apply)

- 1.) Your privacy
- 2.) The safety of your personal information online
- 3.) Other (please explain)
- 4.) _____
Not applicable – I still use the same online services

Feedback about attitudes and concerns

Q20. As a result of the incident related to the complaint you filed, has your attitude towards the government changed? If so, please explain how.

Q21. When you consider interacting with government, do you have any concerns about the trustworthiness of the way the government handles your personal information? Please explain briefly.

APPENDIX D: Protocol for Conducting Survey of Complainants

In order to seek information from complainants, while honoring each individual's right to privacy, a protocol was designed with the Office of the Privacy Commissioner (OPC).

The related requirements included:

- No information would be provided to the researchers by the OPC.
- No complainant would be contacted for the sole purpose of asking them to participate in this research.
- Any complainant wishing to participate would be required to opt-in to the survey and send their contact information to the researchers.

The final protocol:

1. At the completion of a complainant's case, the following was sent to the complainant from the OPC: information from the OPC about the status of the individual's case, a letter notifying the individual that this research was being conducted, and a pre-paid and addressed envelope to send their contact details to the researchers if they wanted to participate.⁷²
2. Complainants, upon receiving notification and details about the study and survey, decided whether or not to opt-in to participate in this project.
3. When a complainant contacted the researchers (always via post or email) and requested a survey, they were sent: an information sheet, a survey, a voucher draw ticket (incentive), and another pre-paid and addressed envelope for returning the completed survey.

⁷² The researchers provided pre-paid and pre-addressed envelopes to the OPC.

APPENDIX E: Interview Questions (Group Representatives)

NB: The word “**individuals**” used in this document refers to the **individuals that the interviewee represents**. The semi-structured nature of the interview will allow for adaptation of questions to the specific group in concern.

Introduction, explain objective of the interview and answer any queries about the project.

1. As far as you are aware, how would you describe the level of trust [**individuals**] have in the government – how trustworthy do they feel the government is?

2. To your knowledge, are there specific concerns that [**individuals**] have about how their personal information is handled by organizations (specifically government organizations)?

3. Do [**individuals**] generally know whether there are any laws or organizations that help to protect their right to privacy?

4. Considering the people you’re representing, do you believe that [**individuals**] have a unique perspective on how their personal info is
 1. Collected (How, For what, How often)
 2. Processed
 3. Stored
 4. Disclosed or accessed
 5. Retained - How long?

5. With regard to [**individuals**]’ personal information, do you believe that they feel more confident that their information will be handled properly by GOVERNMENT organizations or PRIVATE organizations?
 - They need to fill out a form w/ (MSD, IRD, WINZ, ACC, DOL, etc.)
 - They need to fill out a form w/ (bank, supermarket, store, supplier, etc.)

6. As far as you are aware, when [**individuals**] think about the possibility that they'll be able to do things ONLINE (e.g., interact with government) instead of other means, do they think that this will alleviate concerns / make them feel more comfortable / confident, or exacerbate the situation and their concerns?

7. Considering the individuals you are representing, how likely are [**individuals**] to use online services that require them to give personal information?

8. Do you know whether [**individuals**] have heard any stories in the MEDIA about privacy issues / problems – people's personal information being lost / disclosed improperly / mis-handled? If so, do you know whether these have had any effect on people?

Follow-Up (depending on answer of 8) If there were stories in the MEDIA about this, do you believe it would affect [**individuals**'] concerns about how personal information is handled – or their willingness to provide information to organizations?

9. As far as you are aware, do [**individuals**] ever make a fuss about giving information - or refuse saying they don't want to or don't think you should have to?

10. Are there any events (e.g., The Holocaust, Dawn Raids of the 1970s) you are aware of that affect [**individuals**'] views / concerns about personal information?

11. As far as you are aware, which channel do you feel [**individuals**] feel the most confidence in when they need to provide personal information to government organizations (in person face to face, by phone, by Internet / email, by postal mail)?

And are there any specific concerns about the trustworthiness of any of these channels?

12. Within the group of New Zealanders you're representing, do [**individuals**] trust some parts of government more than others (politicians / bureaucrats, or different agencies)?

13. Is there anything else that you would like to add about the views [**individuals**] have about privacy and how it relates to their willingness to trust government organizations?

APPENDIX F: Coding Framework

TERM CATEGORIES	CODE TERM / PHRASE
Definitions (of privacy)	General definition
	In terms of type of info (i.e., defining in terms of the type of info)
	In terms of personal reputation
Government	Role of Government
	Responsibility of Government / social contract
	Power relationship - choice
	Different agencies - perceptions / level of trust
	Policies (in place, observed)
	Need for information
	Data Matching / Sharing
Private Organizations	Perceptions / motivations
	Relationship
	Policies
Social / Personal	Cultural issues
	Small society
	Age / personal circumstances
	Personal beliefs / attitudes
	Reluctance to complain
	Affirmed attitude Vs. Behavior / action
	Willingness to provide info
Information Processing / Storage	Control of information flow
	Access to information (once provided)
	Understanding (or lack thereof)
Consequences of Breach	Type of info (health, finances, family, associations, contact, etc.)
	Cause of breach (mistake, incompetence, systemic, deliberate)
	Assignment of blame - individual or organization
	Punishment for wrongdoers
	Organizational honesty
	Number of occurrences (one-off or not)
Channel	Confidence / Trustworthiness
	Channel relationship
	Ability to check / see what's recorded
	Benefits of channel (e.g., record of event)
Anecdotes	Personal (first hand experience, word of mouth)
	Media
Technology	Concerns (general, Internet, security)
	Personal Experiences online
	Experience issues - lack of understanding
Recurring Issues	Unsolicited contact - (phone calls, mail, spam)
	ID theft
	National ID cards
	Name Suppression
	Expectations
	Privacy Act awareness