TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI
VICTORIA
UNIVERSITY OF WELLINGTON

Public Attitudes to the Sharing of Personal Information in the Course of Online Public Service Provision

Final Report

Professor Miriam Lips, Dr Elizabeth Eppel,
Amanda Cunningham & Virginia Hopkins-Burns

Victoria University of Wellington
August 2010

This report is publically available and can be downloaded from the following URL: http://e-government.vuw.ac.nz/summary_IRD.aspx

Acknowledgements

This research project has been led by Dr Miriam Lips, Professor of e-Government at Victoria University of Wellington (VUW), and conducted in partnership with Inland Revenue Department (IR) and Colmar Brunton. Researchers involved in this project are Professor Miriam Lips (VUW) and Dr Elizabeth Eppel (VUW), with support from Amanda Cunningham (VUW) and Virginia Hopkins-Burns (IR). The focus groups have been organised and facilitated by Colmar Brunton. A Project Advisory Group has been established for this project, including representatives from the Inland Revenue Department, Ministry of Social Development, State Services Commission, and the Office of the Privacy Commissioner.

The research project has been financially sponsored by IR and the sponsors of the VUW Chair in e-Government: Victoria University of Wellington, Datacom Systems Ltd, State Services Commission, Department of Internal Affairs, FX Networks Ltd and Microsoft New Zealand Ltd.

The Chair in e-Government would like to acknowledge the research participants, Inland Revenue Department, Colmar Brunton, Victoria University of Wellington, Datacom Systems Ltd, State Services Commission, Department of Internal Affairs, FX Networks Ltd and Microsoft New Zealand Ltd., and the Members of the Project Advisory Group for their valuable input and support to this research activity.

ISBN 978-0-4751235-6-5

Executive Summary

The desire of government and its agencies to develop new online forms of integrated service provision to citizens requires an increased sharing of personal information between individuals and government agencies and across government and, with that, touches upon the citizen's right to privacy. In this study, we used a qualitative research approach to more deeply explore attitudes of New Zealanders towards the collection, management, and sharing of personal information in the course of electronic public service provision.

The research methods used in this project were a review of available international and national research in the field, semi-structured interviews with IR staff about the conditions and future directions of online integrated public service provision, and ten intensive focus group meetings with different members of the general public and across New Zealand, in May – June 2010. In total, 63 individuals participated in the focus groups. The focus group meetings were prepared and conducted in partnership with Colmar Brunton. For further information on the research design including the limitations of this research, the analytical framework developed for this project, and characteristics of the focus group participants and discussions, please see chapters 2, 3 and 4 of the full report. A detailed description of the research findings can be found in chapters 4, 5 and 6 of the full report.

A summary of the main research findings

Our research findings demonstrate that the majority of participants had a benign view of information sharing intentions and practice in the New Zealand public sector. Generally, the participants in this study had a high trust in the New Zealand government and its agencies and thought that they are working in the best interests of citizens. Exceptions could be found among participants with a high dependency on social services; Māori; Pasifika; and self-employed participants.

In general, our research population turned out to be privacy pragmatists: individuals who are prepared to provide personal information to organisations in return for enhancements of public service provision or other personal or collective benefits. However, our research participants were not unconcerned about their privacy and clearly pointed at the need for public service agencies to play privacy by the rules by using provided information only for the intended purpose and asking clients for consent.

Transparency about the use of their personal information by government agencies was generally absent amongst our research participants. Participants provided their information to public sector agencies in order to get the service, but they usually did not understand how their information will be processed or used; why they need to fill in multiple forms with the same information; how and to what length their information will be stored or kept; and who will have access to their information, for instance.

Furthermore, participants showed limited knowledge about the sharing - or non-sharing - of information between agencies. An area of concern to a number of research participants was the accuracy of personal information stored and processed by government agencies, and particularly information used for categorising clients and determining eligibility for services. Several research participants noted problems with incompetent frontline staff members making mistakes with the handling and processing of personal information. This lack of transparency and perceived administrative incompetence led participants to feel uncomfortable about information sharing and wanting to have more control over

personal information provided to public sector agencies. This particular response was stronger among those participants who were more distrustful of government agencies, such as participants from the self-employed, Pasifika, Māori, and beneficiary groups.

A tension in participants' perspectives could be observed in discussing the advantages and disadvantages of cross-agency information sharing at a collective level of interest, and at a personal level of interest. From a collective interest point of view, the majority of participants saw clear benefits of cross-agency information sharing, such as increased effectiveness in public service provision to individuals and a fair allocation of taxpayer funded services, and were permissive therefore. Several participants also pointed at advantages of cross-agency information sharing at a personal level, such as simple and convenient public services, fair public service provision for those who play the game in accordance with the rules, and efficient public service provision.

Where participants perceived disadvantages of cross-agency information sharing at a personal level of interest, they tended to be more protective of their personal information and pointed at the requirement of privacy protection. For instance, vulnerable individuals, particularly those highly dependent on social services, tended to regard information that could be used against them, or information that might lead to a misjudgement in public service provision, as private information. Other high users of social services, such as the super-annuitants, thought they were being asked too much private information and felt they did not have any choice about providing the requested information as they needed the service. Furthermore, participants generally felt uncomfortable in sharing personal information with agencies with an eligibility monitoring function and powers to force compliance.

There were also concerns that frontline staff members were not asking for the relevant information to provide the right service. Furthermore, participants expressed difficulties in finding and joining up the bits of public service information that are relevant to them. Research participants experienced limitations of standardised form filling, and a lack of relevant and integrated public service information in accessing public services online. For some, the lack of provision for adding relevant information to their individual case in an online form was the reason they preferred to speak to a staff member rather than using the e-channel for public service consumption.

Most of our research participants demonstrated attributes belonging to a Service State perspective in their attitudes towards information sharing, such as better public service provision and increased service effectiveness; only some of them showed attributes of a Surveillance State perspective, such as increased information asymmetries, eroded trust, social sorting and putting people in the wrong box.

We also observed that, although research participants generally support cross-agency information sharing for the achievement of a Service State perspective, they did not see specific attributes of a Service State perspective, such as reduced duplication, holistic needs-based service provision and improved access to public services, in the public service relationships they have experienced thus far. Instead, research participants referred to attributes which neither belong to a Service State perspective nor a Surveillance State perspective. These attributes appear to constitute an alternative scenario among our research participants, a Fair State perspective in which increased use of Internet service channels lead to more efficient systems and value for money for the taxpayer; more efficient and equitable enforcement; more fairness in public service use; improved decision making by government

agencies; improved service administration by agencies; reduction in information asymmetries; and equality under the Law.

Towards a contextual integrity approach of information sharing

Our research findings strongly support the theoretical viewpoint that context determines peoples' attitudes towards information sharing and privacy in public service environments. The following context-related factors appeared to be of particular importance among our research participants.

Firstly, we observed substantial differences between the majority of our research population and specific groups within that population. We noted differences in information sharing attitudes of those participants with high service dependence; participants who are self-employed; Māori participants; and Pasifika participants. For instance, high service dependent participants and those who are self-employed perceived all personal information as private information, and only wanted to share information with government reluctantly and if they have to, as government is 'not working for them'. Furthermore, high service dependent participants saw clear negative power imbalances and information asymmetries between themselves and public sector agencies. These negative feelings of distrust and powerlessness towards public sector agencies were also present among Māori and Pasifika participants with some subtle differences: for instance, whereas Māori particularly were negative about the integrity and Māori language use of individual public service staff members, Pasifika people found dealing with government agencies difficult and felt demeaned by the process.

Secondly, participants generally supported information sharing between agencies with close or related mandates and overlapping responsibilities. Roughly, we observed that participants make a distinction between the following service clusters: a financial service cluster (e.g. IR & ACC), a social service cluster (e.g. WINZ & Housing), a justice service cluster (e.g. Police, Courts, Immigration & Justice) and a health service cluster. Underlying reasons for participants to be supportive of cross-government information sharing within these service clusters are that agencies can help each other and do a better job.

Thirdly, participants did not treat public service channels as separate contexts for information sharing, but perceived the public service context for information sharing at the level of their particular service need. We can conclude from this that there can be a tension between participants' 'horizontal' attitudes towards information sharing for the purpose of meeting their service need and the 'vertical' organisation and focus of public sector agencies in public service provision.

Finally, due to the fact that participants often perceived a lack of transparency around information sharing with and between public sector agencies, they also did not have a clear context in which they share personal information with public sector agencies. This situation increased discomfort amongst participants, including feelings of information asymmetries and a lack of control over personal information. Consequently, participants' attitudes towards information sharing and privacy implications were coloured as a result of unclear contextual boundaries for information sharing practice and lacking knowledge on the integrity of personal information shared with public sector agencies.

Based on these research findings, we suggest that a contextual approach should be taken in the design and development of information sharing in the course of e-government service provision. If public

sector agencies would like to achieve a Service State Perspective in the citizens they interact with, a different approach of contextual integrity of information sharing needs to be developed and managed for the following clusters and sectors:

- Information sharing integrity and transparency within clear contextual boundaries for information sharing practice;
- Information sharing integrity within the context of a specific customer target group, such as beneficiaries, Māori, Pasifika, or self-employed;
- Information sharing integrity within the context of a specific service cluster, such as a financial service cluster, social service cluster, justice service cluster or health service cluster;
- Information sharing integrity within the context of a multi-channel-strategy; and
- Information sharing integrity within the context of a customer's service need

Table of Contents

List of Figures

List of Tables

1. Introduction

Governments are exploring ways to develop new online forms of integrated public service provision to citizens. With the need to shift from real world, personal interactions between customers and public sector agencies to digital, information-based interactions, this new public service model would require an increased sharing of citizens' personal information between agencies in the back-office of online public service provision. Expected benefits of this new e-service model are many and varied and include increased effectiveness of public service provision (e.g. tailor-made service provision to individuals); increased efficiency and reduced costs; improved convenience; improved ease of contact between citizens and government; and improved monitoring to ensure compliance, equitable enforcement, exclusion of unwanted individuals and activities, or enhanced personal and public protection.

One of the New Zealand government departments that have adopted and want to further develop this new public service model is the Inland Revenue Department (IR). In the future, according to IR's strategic intentions, IR customers will experience a shift from paper-based service provision to service delivery via the Internet. Furthermore, the intention is to increase the offering of integrated e-services to individuals. These strategic intentions support IR's strategic goal that, by 2014, IR will:

> "Make it easy for customers to self-manage their obligations and receive their entitlements through simple, clear information, and … use straight forward self-service systems":
>
> - We will reduce the burden on our customers;
> - We only collect the information we really need;
> - Improve efficiency and reduce cost; and
> - Streamline, automate and integrate systems, processes and tools"

However, the collection, processing and sharing of personal information required to achieve this new e-service model touch upon a fundamental right of citizens: the right of privacy. Privacy is a multifaceted, ambiguous notion which means many things to many people. For instance, people from different cultures attach a different meaning to this concept (Moore, 1984). Moreover, what is considered 'sensitive' personal information varies with context and in relationships. Furthermore, the meaning of privacy is changing under the possibilities opened up by new Information and Communication Technologies (ICTs), with younger generations, as digital 'natives', developing different perceptions of privacy compared to older generations (Madden & Smith, 2010).

So far, the information available about people's attitudes towards the sharing of personal information in these new electronic public service relationships, and the implications for their privacy is limited. In this research project, we used a qualitative research approach to more deeply explore attitudes of New Zealanders towards the disclosure, collection, management, and sharing of personal information in the course of electronic public service provision.

2. Research Design

2.1 Research motivation and objective

Privacy and particularly the notion of 'personal information' have become complex and ambiguous concepts in an information age in which service relationships between individuals and government are increasingly based on the exchange of digital information instead of real world interactions. How society has changed becomes particularly clear if we compare our current issues around privacy and the sharing of personal information with the end of the 19th Century, when Warren and Brandeis published their seminal article on The Right to Privacy (1890). In that article, they observed substantial privacy issues as a result of "snapshot photography", a novelty at the time that created an opportunity for newspapers to publish photographs of individuals without their consent. Warren and Brandeis argued that private individuals were being continually injured and that the practice weakened the moral standards of society as a whole (Warren & Brandeis, 1890).

Since then, the meanings of privacy, 'personal information' and information sharing seem to have changed considerably as a result of the introduction and use of new Information and Communication technologies (ICTs) in society. In the public sector for instance, ICTs are increasingly used for service transformation and the development of integrated e-government service relationships with the citizen, which require the collection, processing, storage, sharing and use of (new forms of) citizen identity information. With that, in developing more efficient and effective public services, public sector agencies are becoming more dependent on citizens and their willingness to share personal information in new e-government service environments.

This development raises important questions about what peoples' attitudes are towards the disclosure, collection, management, and sharing of personal information in these new electronic public service relationships, and the implications for their privacy. Thus far, there is not much empirical, in-depth knowledge available in this area. The knowledge we have usually is collected via quantitative surveys with a tendency to focus on concerns people have with regard to their privacy in a societal environment that is rapidly changing as a result of the adoption of new technologies (Bennett & Raab, 2003). Moreover, acknowledging that people may have varying attitudes towards privacy and information sharing in different online public service environments, there is not much qualitative data available about attitudes from different members of the general public involved in varying public service relationships. Furthermore, the unique relationship between citizens and government may lead to different attitudes about the sharing of information in public service relationships, compared to information sharing with commercial organisations, for instance. Also, there is not much empirical evidence on what peoples' attitudes are towards information sharing in new integrated e-government service environments with multiple public sector organisations involved in the back-office of the e-service channel. This study aims to broadly and deeply explore attitudes of different members of the New Zealand general public towards the sharing of personal information with and across public sector agencies in online public service environments.

2.2 Research question

The research focused on the following question:

What are attitudes of different members of the New Zealand general public towards the collection, management, and sharing of personal information in the course of online public service provision?

2.3 Research approach and methodology

In order to find answers to this research question we used a qualitative research approach to empirically explore attitudes of a variety of New Zealanders in their service relationships with New Zealand public sector organisations. The research was conducted from March 2010 until August 2010, using the following research methods:

- A review of international and New Zealand-based literature in the area of information sharing, privacy, and the management of citizen identity information in e-government service environments;
- Semi-structured interviews with New Zealand public sector staff about the characteristics, conditions, and strategic developments in online integrated public service provision in the New Zealand public sector;
- Ten focus groups with representatives of the New Zealand general public.

Firstly, we wanted to establish the factors that potentially influence the attitudes of individuals towards the sharing of personal information in the course of online public service provision. We therefore conducted a review of available academic and professional literature in the broader field, with a particular interest in empirical research findings and theoretical insights derived from qualitative research. On the basis of theoretical assumptions presented in available literature we developed a set of analytical themes of relevance to our research. An overview of the relevant analytical themes, the underlying theoretical assumptions and a further explanation of these theoretical assumptions in the literature are presented in Chapter 3 of this report.

Secondly, we 'translated' the analytical framework into a list of sample criteria for our research population and a list of information areas, or 'Topic Guide', we wanted to further explore in each focus group meeting with different groups of representatives of the New Zealand general public. This empirical phase of the research activity was developed and conducted in partnership with Colmar Brunton. In order to further shape the identified information areas and explore realistic scenarios of information sharing situations in different online public service environments with research participants, we conducted five semi-structured interviews with IR staff about characteristics, conditions, and strategic developments in online integrated public service provision.

Ten focus group meetings were organised and conducted across New Zealand, in May/June 2010, with each focus group involving six to eight participants in an in-depth collective discussion of about 2.5 hours based on the Topic Guide. We identified the following sample criteria for focus group participants: age, gender, ethnicity, income, employment, public service dependency, education level, geographic location, Internet use, and e-government service use. We also wanted to include in our sample population individuals with an experience of online integrated public service provision, such as tertiary

students who have experience with integrated student loan services online, and individuals who are highly dependent on (integrated) public services, such as benefit recipients. In total, 63 individuals participated in the focus groups. Further details about the focus group participants, the profile of each focus group and the distinctive flavour of the discussion in each focus group, are provided in Chapter 4 of this report.

2.4 Limitations and delimitations of the research

This research activity used an in-depth qualitative research approach involving a relatively small research population of 63 members of the New Zealand general public. The ten focus groups were purposely and with maximum variation sampled on the basis of a list of selection criteria to gain a high quality, detailed understanding of information-rich group discussions (Patton, 2002). Although this particular research design decision creates opportunities of gaining in-depth understanding of each group of members of the New Zealand general public and exploring important shared patterns that cut across individual research participants, it also creates limitations regarding generalisation of the research findings. We present some further details about the (limited) representativeness of the total research population of this study in Section 5.1 of this report.

Another limitation is the fact that attitudes of individual research participants might be influenced as a result of processes of 'group think': group discussions and other information exchange in the focus group meeting might have developed, shaped and even changed the attitude of an individual participant. Indications that some 'group think' might have happened in our focus groups are final comments made by a few research participants like "I learned a lot tonight". Furthermore, due to several group assignments during the focus group meetings, such as the discussion of information sharing scenarios or the sorting of cards with names of New Zealand government agencies, some of the research findings are clearly group outcomes, instead of opinions or attitudes of individual participants. Consequently, in the reporting of our research findings, we sometimes attribute research findings to certain focus groups rather than to individual participants. A further limitation of this research is that focus groups to some extent had different discussions, which has implications for the comparability of research findings across the focus groups.

A delimitation of the research is that we have only explored peoples' attitudes towards information sharing and privacy in the course of online public service provision, and not peoples' actual online behaviour. As available research suggests that there can be substantial deviations between what people say and what they actually do online, we acknowledge a need for further research in this particular area.

3. Analytical Framework

3.1 Introduction

According to available literature, the following analytical themes need to be considered in relationship to attitudes of members of the general public towards the sharing of personal information in the course of e-government service provision. Each of these themes covers theoretical assumptions derived from the literature and indicating a potential impact on attitudes of individuals towards information sharing with and across government. Generally, a distinction can be made between analytical themes based on demographic characteristics of members of the general public, and more general themes derived from international literature. We first provide an overview of all the themes considered in this research and then discuss the themes more in detail.

Analytical themes related to the following demographic characteristics:

- Age
- Culture/Ethnicity
- Geographical Location/Community
- Employment
- Level of Income
- Education

General analytical themes:

- Individuals' acceptance and use of the Internet
- Channel choice
- Trust in government and/or the public service providing organisation
- Information sharing:
  a. Information relationship between the individual and the public sector
  b. cross-government information sharing
  c. implications of information sharing
- Informational privacy
- Trust in the e-service environment: information security
- Awareness
- Experience, skills, ease of use
- Transparency/openness

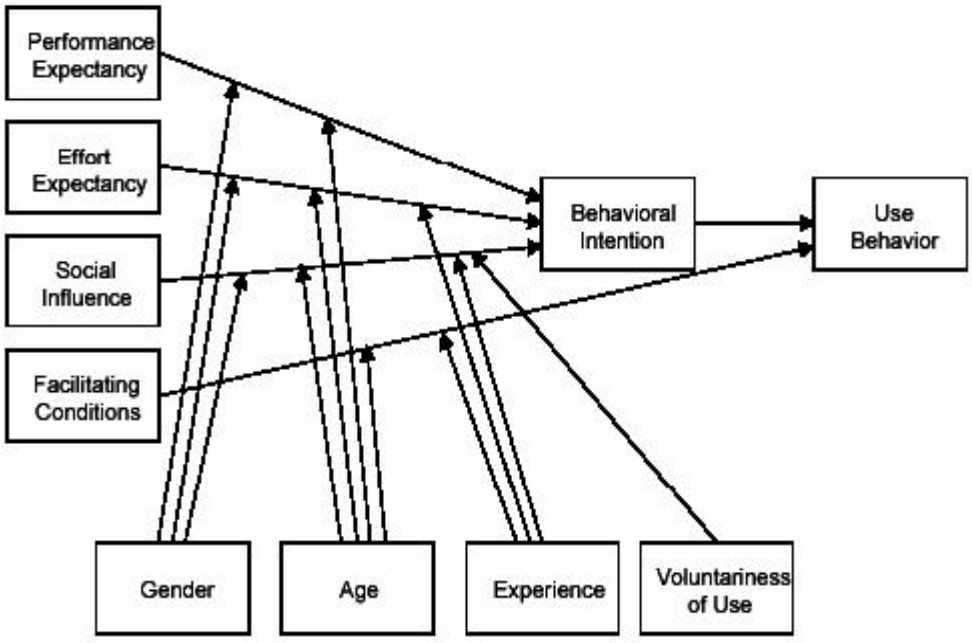
3.2 Analytical themes related to demographic characteristics

A theory which aims to explain the intentions of individuals to use the Internet, and subsequent usage behaviour, is the Unified Theory of Acceptance and Use of Technology (UTAUT). According to this theory, ICT usage intentions and behaviour are determined by the following four constructs (Venkatesh, Morris, Davis, & Davis, 2003):

- *Performance Expectancy*: perceived usefulness of the technology or the degree to which an individual believes that using the technology will help him or her to attain gains in job performance;
- *Effort Expectancy*: perceived ease of use of the technology
- *Social Influence and Factors*: social background, socio-cultural norms and values of an individual;
- *Facilitating Conditions*: perceived technical and organisational support, perceived behavioural control of an individual

The variables of gender, age, experience and voluntariness of use moderate the key relationships in this model (see Figure 1).

Figure 1 - Diagram of the Unified Theory of Acceptance and Use of Technology (UTAUT)



Source: Venkatesh *et al*. (2003, p.447)

In this research activity, we have used constructs and variables of the UTAUT-model to explore the attitudes and intentions of individuals regarding Internet use in public service relationships. As we didn't study the actual behaviours of individuals in this research activity, we didn't focus specifically on the constructs of facilitating conditions and, to a lesser extent, performance expectancy. The construct of effort expectancy has been covered under the general theme of 'ease of use' in this study. Further, voluntariness of use has been explored through the theoretical assumption of Internet use, non-use and ex-use. Under the construct of Social Influence and Factors, we explored demographic characteristics with a possible effect on the attitudes of research participants to information sharing in the course of online public service provision. The following findings from available research further demonstrate the need to consider the listed demographic characteristics as variables in our study.

3.2.1 Age

Research suggests that youth have different perceptions of informational privacy compared to older generations (Livingstone & Bober, 2004; Madden & Smith, 2010; Palfrey & Gasser, 2008).

In New Zealand, in December 2009, 80 percent of individuals over 15 years had used the Internet in the last 12 months compared with 69 percent in 2006. The highest users were 25-44 year olds (56 percent) followed 45–64 year olds (44 percent), 15–25 year olds (40 percent), 65–74 year olds (20 percent) and 75+ year olds (6 percent) (Madden & Smith, 2010; Statistics New Zealand, 2010)

Based on the opinions of more than 5000 European youth (15—25), Lusoli and Miltgen (2009) note that young people are sceptical of the internet as an environment for the exchange of private data, and have major doubts about personal information protection. A recent US-based study (Madden & Smith, 2010, p. 2) also found that young adults are generally less trusting of the sites that host their content. For instance, when asked how much of the time they think they can trust social networking sites like Facebook, MySpace and LinkedIn, 28 percent of users aged 18-29 say "never." By comparison, fewer older users express such cautious views: 19 percent of users aged 30-49 and 14 percent of those ages 50-64 say they never trust the sites. Krasnova and colleagues (Krasnova, Gunther, Spiekermann, & Koroleva, 2009) have found young people tend not to supply private information in the face of privacy concerns.

3.2.2 Culture

A 2009 Survey into Internet use of New Zealanders (Smith, *et al*., 2010, pp. 34, 44) shows that about 95 percent of Pakeha and Asian New Zealanders use the Internet at home, while about 80 percent of Maori and Pasifika do so. Asians are significantly more likely (approx 95 percent) to rate the Internet as important in daily life, than Pasifika (approx 67 percent), Pakeha (approx 53 percent) or Maori (approx 48 percent).

3.2.3 Location/Community

The same NZ survey of Internet use (Smith, *et al*., 2010) found that Internet usage in this country can be correlated to geographical location as well as size of the local community. Differences particularly can be found between the three major local communities in New Zealand, i.e. Auckland, Wellington and Christchurch, and the more rural areas. For example, 88 percent of the population from the three major centres have broadband at home, compared to 67 percent of rural New Zealanders (Smith, *et al*., 2010, pp. 30, 31). Another example is that 53 percent of city dwellers belong to a social networking site compared to 31 percent of rural New Zealanders. Furthermore, the 2009 survey findings demonstrate that, in terms of their Internet usability, around 55 percent of urban New Zealanders rate themselves at a good to excellent level, compared to around 35 percent of rural New Zealanders.

3.2.4 Level of income

In a recent New Zealand study, those respondents categorised by the $10,000-$20,000 and $20,000-$30,000 income ranges were significantly less likely to have used the Internet – for any activities – in

the previous 12 months than those in higher income groupings. The primary reason for this was access: 65 percent of the participants did not have a computer; 30 percent did not have Internet access, and 35 percent were not comfortable using the Internet (State Services Commission, 2010).

3.3 Theoretical assumptions per general analytical theme

3.3.1 Individuals' acceptance and use of the Internet

1. Scholars generally make a distinction between Internet users, non-users, and ex-users.

In accordance with the Unified Theory of Acceptance and Use of Technology (UTAUT), an individual's acceptance of technology and more specifically the Internet, can be understood in terms of Internet use behaviour. In the literature, a common distinction is made between individuals who are using the Internet or Internet users, individuals who are not using the Internet or Internet non-users, and individuals who have used the Internet in the past but are not using it nowadays or Internet ex-users (see, for example, Dutton, Helsper, & Gerber, 2009; Smith, *et al*., 2010). With regard to Internet users, a further distinction is often made between individuals who are making intensive use of the Internet, i.e. high users, and individuals who use the Internet on a regular basis but not every day, i.e. low users. For instance, the Eurostat survey on Internet use by individuals living in the European Union makes a distinction between high users, or individuals who are using the Internet at least daily, and low users, or individuals who are using the Internet at least weekly (Eurostat Information Society Statistics 2009). Ex-Internet users can have various reasons for not using the Internet any longer. For example in the UK, in 2009, ex-Internet users indicated that the main reason for not using the Internet any longer are the costs involved (Dutton, *et al*., 2009).

Internationally and over time, many research initiatives have indicated the emergence or existence of a so-called 'digital divide'. In general, the digital divide refers to the gap between individuals who have access to the Internet and are using it, and those who do not have Internet access and are not using it (e.g. OECD, 2001). However, Norris (2001) points out that the term 'Digital Divide' has become a popular term for each and every inequality related to Internet access or community development. She therefore prefers to understand this concept as a multidimensional phenomenon encompassing the following three aspects in her view (Norris, 2001, p. 4):

- the *global divide*: the divergence of Internet access between industrialised and developing societies;
- the *social divide*: the gap between information rich and information poor in each nation; and
- within the online community, the *democratic* divide: the difference between those who do, and do not, use the panoply of digital resources to engage, mobilise, and participate in public life.

Similarly, other scholars too acknowledge the multiple dimensions of this phenomenon and generally make distinctions between an access or socio-economic divide, and a skills or usability divide (see for instance Mossberger *et al*. 2008; Van Dijk, 2005).

A New Zealand Internet study (Smith, *et al*., 2010, p. 3) shows the extent to which the Internet has become an integral part of the lives of the majority of the population. For instance, in 2009, 83 percent of the New Zealand population used the Internet; of the remaining 17 percent who did not use the Internet in 2009, about two thirds had never used the Internet, and about one third was ex-users. Furthermore, in 2009, 40 percent of all users spent at least 10 hours a week on the Internet, with the remaining 60 percent being online for less than 10 hours a week. About 40 percent of all ex-users said they had used the Internet for more than two years before giving it up (*ibid*. 2010, p. 7).

The main reason for the non-users in the 2009 survey was that they did not find using the Internet interesting or useful (42 percent). About one third of all non-users reported to have asked another person to do something for them on the Internet (Smith, *et al*., 2010, p. 6). Furthermore, the New Zealand survey points at a clear economic divide between Internet users and non-users in 2009: only 2 percent of those earning $100,000 or more per year did not use the Internet in 2009, compared to 35 percent of those earning less than $40,000 (*ibid* p. 32).

In 2009, younger New Zealanders used the Internet more frequently and had more positive attitudes towards the Internet compared to older New Zealanders (*ibid*, p. 26). The 2009 survey also shows that a person's gender plays a lesser role than some other demographic characteristics in determining differences: more or less equal numbers of males and females, just over 80 percent, used the Internet in 2009 (*ibid*, p. 28).

2. *E-Government researchers commonly distinguish between e-Government service use categories of 1) Looking up public sector information online; 2) Interacting with government agencies online; and 3) doing transactions with government agencies online*

Scholars in the field of e-government commonly make a distinction between the following e-government service use categories (e.g. Andersen & Henriksen, 2006; Millard, 2006):

1. *Information provision*: looking up public sector information online;
2. *Interaction or Communication*: interacting with government agencies online; and
3. *Transaction*: doing transactions with government agencies online

Often these e-government use categories are perceived as a staged model of increased e-government maturity (Andersen & Henriksen, 2006; Layne & Lee, 2001; Yildiz, 2007).

In 2009, New Zealanders accessed public sector information and services via the Internet in significant numbers: about 40 percent looked up public sector information and about 30 percent paid taxes or fines online (Smith, *et al*., 2010, p. 19).

In the same 2009 survey, a significant relationship could be observed between the level of education and the predisposition to use the Internet to get information about public sector services. Moreover, younger generations, especially those in their 30s (77 percent) and 40s (72 percent), were more likely to get information about public services online, compared to older generations. Furthermore, high proportions of New Zealanders with an income starting at $65k (68 percent) and those who live in the three major cities in New Zealand (64 percent) have used the Internet to look up information about public services. In the 2009 survey, demographical characteristics like gender and ethnicity didn't

reveal any substantial differences across the New Zealand population, with an equal balance between males and females (approx 60 percent each) and only slight differences in online information provision amongst ethnic groups (55 – 65 percent) (Smith, *et al*., 2010, p. 56).

The 2009 survey also shows that more than 50 percent of New Zealanders used the Internet for accessing public services. Of the ethnic groups, relatively high numbers of Pasifika reported to have used the Internet for public service consumption (approx 75 percent, compared to approx 52 percent of other ethnicities) (Smith, *et al*., 2010, p. 57).

In another recent New Zealand-based survey, the 2009 Kiwis Count Survey conducted by the State Services Commission (2010), 47 percent of the 3,724 respondents indicated that they had used the Internet in the last 12 months to contact government.

3.3.2 Channel choice

3. Channel choice is driven by the perceived value associated with the channel

Individuals select a public service channel using a variety of criteria and typically balancing 'enablers' and 'barriers'. Channel choice is driven by the perceived value associated with the channel (Broekhuizen & Jager, 2003). Issues involved in this value judgement are utility, price, effort, risk, stress, quality and authenticity, status and exclusivity, and enjoyment and pleasure (*ibid*).

With regard to e-service channels, the following additional issues are of importance to customers in deciding upon a service channel: the reputation of, and trust in, the organisation; 'informativeness'; ease of use or usability; website design; and perceived control (Her Majesty's Revenue and Customs, 2008; Rotchanakitumnuai, 2008; Torgler, 2007). For customers of services offered by tax administrations, the following issues play a role in decisions around channel choice: the customer's comfort, reliance and trust with using existing channels; not being technologically confident or knowledgeable; not having access to appropriate technology; and not trusting the online transaction system (Kelly & Hopkins-Burns, 2010).

In 2005, a large European survey into user attitudes to e-government services found that individuals anticipate experiencing the following barriers to using e-government services: difficulties in starting to use the e-government service, including a feeling that face-to-face service provision is better; and fears around the privacy of their personal data (Millard, 2006). However, the same survey also found that, once citizens of the 10 European Union member states included in the study have used e-government services, they perceive lower barriers to e-government service use, and mainly related to the feeling of being left alone with service-related problems or questions (*ibid*).

In New Zealand, of the non-Internet users surveyed in the 2009 Kiwis Count Survey, half reported nothing would encourage them to access government services online (State Services Commission, 2010). Further, of those that had used the face-to-face channel for service, 34 percent reported they would still use this channel despite other channels available to them.

4. Online channel adoption is influenced by trust

Online channel adoption is influenced by trust in the e-environment (e.g. Camp, 2003; Connolly & Bannister, 2007; please also see Section 3.3.7). To explore how trust influences the adoption of online channels, Backhouse & Halperin (2006) took a high level conceptualisation of trust as a three part concept involving a truster, attributes of a trustee, and a specific context over which trust is conferred. Their context was the possible introduction of an eID scheme for the EU. According to their study, trust in online channels depends on:

a. Trust in governance (e.g. "I believe my interests will be represented in deciding how digitised personal data will be exchanged");
b. Trust in Policy (e.g. "I believe there will be an appropriate legal environment to regulate how my personal data with be exchanged");
c. Trust in Monitoring (e.g. "I believe that personal data exchange will be monitored by competent authorities");
d. Trust in Security (e.g. "I believe that the systems used by authorities to issue and manage ID cards will not be technically secure");
e. Understanding (e.g. "I understand I will be able to assess the benefits when allowing my personal data to be shared by ID authorities");
f. Ease of use (e.g. "I feel that I will find electronic ID cards difficult to use"); and
g. Usefulness (e.g. "I understand the need to exchange my personal data across government departments; between government and business; and across different countries").

A New Zealand-based study into customer satisfaction with e-services provided by the Inland Revenue Department (IR) found that IR customers considered trust in IR, its processes, its website and its information security, important drivers to use the e-channel (National Research Unit, 2009).

5. Individuals often use multiple channels to access public services

The research findings of the 2009 Kiwis Count Survey show that New Zealanders use multiple channels to access government services (State Services Commission, 2010). For example, when looking for information about government services, just as many of the survey participants use the telephone as the Internet (55 percent respectively), 35 percent use face-to-face service, and 16 percent use mail or fax. Similarly, for transactions with government departments, face-to-face is used by 54 percent of respondents, telephone by 51 percent, the Internet by 40 percent, and mail or fax by 27 percent. Other key findings of the 2009 Kiwis Count Survey include:

- the Internet is the most preferred channel to obtain information about government services, face-to-face service is preferred when conducting transactions, and telephone is the second most popular channel for both these tasks;
- Customer satisfaction is highest with face-to-face service (an overall average of 79 percent), followed by the Internet (approximately 63 percent), and telephone (60 percent);

- Customers who use the Internet for accessing public services are more likely to report they would use that service again, compared to users of telephone or face-to-face based services; and
- Internet-based public services are best targeted to those customers aged under 65, as older customers are less able to, and less interested in, accessing government services online.

When asked what would encourage respondents to use e-government service channels, the most common responses were to make online services simple and user-friendly; to provide follow-up confirmation to avoid misunderstandings; ensure privacy is protected; and to improve online security (State Services Commission, 2010).

The 2009 Kiwis Count Survey also included questions about mobile phone use in the course of public service provision (State Services Commission, 2010). The research findings suggest that mobile phones are becoming an acceptable way to access and/or receive public services: for instance, 10 percent of the respondents indicated they have already sent or received text messages from a government agency, 39 percent have dialled a free phone number from a cell-phone to access public services, and 36 percent of the respondents said they would dial a free phone number from a cell-phone to access public services; however, 53 percent of the respondents indicated they would not use their mobile phone to access a government website (*ibid*, p. 3). Compared to other ethnic groups, Maori and Pasifika respondents were more likely to support using mobile phones to access public services.

A 2009 New Zealand-based study found that IR customers expect future IR services to become more streamlined, simple, and easy to understand, and that more services will be available online (National Research Unit, 2009) Also, there is an expectation that customers will be able to online access their own personalised and secure accounts detailing their service obligations. The 2009 study shows that IR customers perceive the use of email as inevitable and desirable to make the online interaction 'more human'. Email was particularly considered useful to confirm transactions and as an avenue for having queries resolved. Participants also suggested chat boxes as an appropriate tool for answering generic questions. Texting via mobile phone was seen as an inappropriate channel for interacting with the Inland Revenue Department; however, there was support for receiving text reminders when deadlines are imminent. Furthermore, respondents viewed the use of video-communication as an online channel for tax-related services less favourably, based on perceptions of not being able to get access to staff. There was some support for downloadable educative material in video format (National Research Unit, 2009, pp. 5-6).

3.3.3 Trust in government and/or the service providing organisation

6. *Citizens' trust in the public service contributes to the broader concept of trust in government. Citizens' trust in government is fluctuating within and across countries, as well as over time*

Internationally, concerns with declining levels of citizens' trust in government and public service provision are featuring prominently in public debate (Castells, 2009). An important reason for this decline in citizens' trust is often perceived to be the lack of government performance (e.g. Barnes & Gill,

2000; Bok, 2001). However, based on an international review of major opinion surveys on citizens' trust in government and public service delivery, including the World Value Surveys and Eurobarometer Surveys, Van de Walle *et al*. (2008) reject this hypothesis of a universal decline of trust in government. Instead, they find that citizens' trust in the public sector is fluctuating within and across countries, as well as over time (Van de Walle *et al*., 2008). Moreover, they point out that attention to attitudes towards public services and public service provision has been very limited in these surveys. From another research project in which they tested the contribution of public service provision to citizens' general opinion of government, Van de Walle *et al*. (2005) conclude that specific evaluations of public service quality can differ substantially from public attitudes towards government, leading to a situation in which low trust in government and a positive image of many specific public services may co-exist.

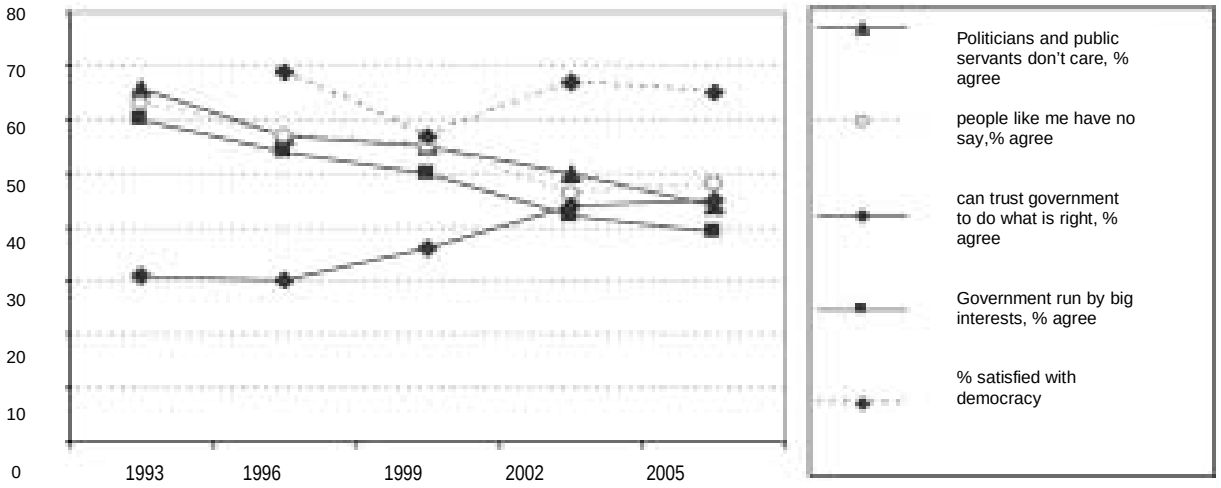
Trust in government goes hand in hand with trust in the public service to:

a. Do what is right;
b. Deliver value for the taxpayer's dollars;
c. Treat citizens fairly (Heintzman & Marson, 2005).

For example, in Canada, the 2008 Canadian Citizens First Survey (Institute for Citizen-Centred Service, 2008) examined the concept of 'confidence in government' via statements put forward to respondents of "I believe the government does a good job" and "I get good value for my tax dollars". The Canadian researchers also investigated the concept of 'confidence in the public service' by having respondents reacting to statements like "I trust the public service to do what's right, and "I can count on the public service to do what is right for citizens". The research findings indicate that citizens' trust in the public service contributes to the broader concept of trust in government: service reputation, service impact, a perception of sound leadership and management of the public service, and a perception that public service is in touch with the needs of the community, all have a positive influence on confidence in the public sector. These perceptions are in turn driven by satisfaction with recent service experiences and a perception of fairness and honesty in the transactions. The drivers of confidence are a complex interplay of the citizen's own experience and information from the media, friends; family and colleagues.

Van de Walle *et al*. (2008) present New Zealand-based research findings on trust in government and democratic institutions, which they derived from available New Zealand Election Study data. While the data are not very detailed and only covering the time period between 1993 and 2005, Van de Walle *et al*. clearly find a positive trend since 1993 (see Figure 2 below): the number of New Zealand citizens saying they can trust their government to do what is right has increased over time, while fewer and fewer citizens think that government is run by big interests or that politicians and public servants don't care (Van de Walle, *et al.,* 2008, pp. 55-56).

Figure 2 - Evolution in trust, New Zealand 1993-2005, in Van de Walle *et al*. (2008, p. 56)



Source: New Zealand Election Study, http://www.nzes.org

A New Zealand-based study of customer satisfaction with e-government services offered by the Inland Revenue Department found trust in IR and its processes on the one hand, and website and information security on the other hand, are important drivers for customer satisfaction. However, IR customers reported they persist with difficulties in e-service interactions – including perceptions of mistrust in the online channel and in the administration – because of the legal obligation to comply with New Zealand's tax and social entitlement laws (National Research Unit, 2009).

7. The key antecedents to trusting behaviour are competence, benevolence, integrity, and transparency

Based on an extensive academic literature search towards characteristics of trustworthiness in relationships between a trusting party and a trusted party (also see Connolly & Bannister, 2007), Bannister presents the following four key antecedents to trusting behaviour (Bannister, 2007, pp. 4-5):

- *Competence*: that group of skills, competencies, and characteristics that enable a party to have influence within some specific domain (cf. Mayer, *et al*., 1995)
- *Benevolence*: the extent to which the trusting party believes that the trusted party wants to do good things (cf. Lee & Turban, 2001)
- *Integrity*: the trusting party's perception that the trusted party will be honest and adhere to an acceptable set of principles (cf. Lee & Turban, 2001)
- *Transparency*: the ability of the trusting party to understand and observe what the trusted party is doing.

8. *An individual's trust in government is related to their own experience of government and public service consumption, personal experiences of family members and friends, and through stories in the media.*

An individual's trust in government is related to their own experience of government and public service consumption, personal experiences of family members and friends, and through stories in the media (Institute for Citizen-Centred Service, 2008; Torgler, 2007). External sources of information are particularly relied upon when the individual is not familiar with the government department and/or with the service: this is for instance the case with regard to the New Zealand tax administration (National Research Unit, 2009).

9. *To public service customers, the impact of a negative experience with a public agency is much more pronounced than the effect of a positive experience*

Empirical research in Belgium on the relation between customer satisfaction with public service delivery and trust in government shows that the impact of a negative experience with a public agency is much more prominent than the effect of a positive experience: put differently, this finding suggests that the breaking down of trust in government and public service provision is much easier to accomplish than the building up of trust (Kampen, *et al.,* 2006, p. 399).The researchers recommend that decreasing the number of disappointed clients will, therefore, have a stronger effect on increasing trust in public service provision and government, than increasing the number of highly satisfied customers.

3.3.5 Information sharing

The literature on information sharing covers the following three discussion areas: 1) Information relationship between the individual and the public sector; 2) Cross-government information sharing; and 3) Implications of information sharing. We further discuss each of these areas below.

3.3.5. Information relationship between the individual and the public sector

10. *An individual can use a variety of personal 'identifiers' to present herself in a public service relationship*

An individual can use a variety of personal 'identifiers' to present herself in a public service relationship, such as a name, address, date of birth, or telephone number (Lips *et al.,*. 2009a; 2009b). Moreover, personal information about an individual is often used for identification purposes during public service provision (Birch, 2007; Camp, 2003; Lips *et al*., 2009a; OECD 2009; Raab, 2005). For example, in New Zealand, the IRD number is a key identifier for an individual in service relationships with the Inland Revenue Department, and between IR and other agencies.

Increasingly, it is unclear what 'personal information' actually means or is (Raab, 2005, 2007). Nissenbaum generally defines personal information as information about an identifiable person (Nissenbaum, 2010, p. 4). According to the New Zealand Privacy Act, 1993, 'personal information'

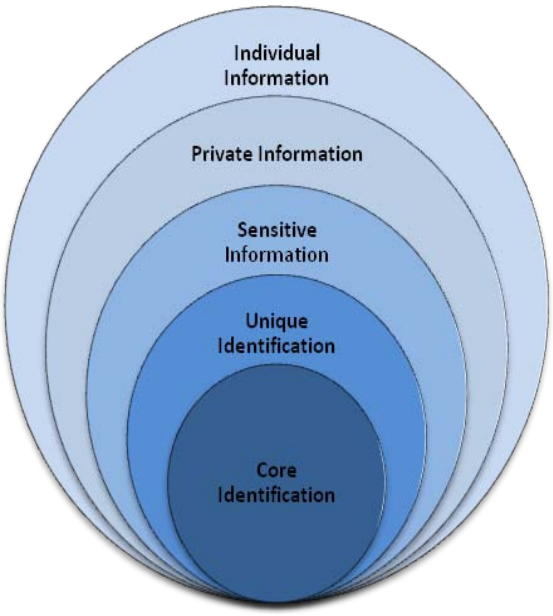
means information about a living human being: the information needs to identify that person, or be capable of identifying that person.

Participants in international studies of public attitudes to privacy and data sharing used a broad understanding of the term. They considered 'personal information' to encompass anything and everything that could be used to identify an individual, or that could be used as a means of obtaining knowledge that an individual considers to be 'private' (Australian Communications and Media Authority, 2009; MORI, 2003).

Marx (2004) uses an integrated vision on varying types of personal information, which he calls 'identity knowledge'. He visualises the relationship between different types of personal information as a set of concentric circles (see Figure 3).

In Marx' model of identity knowledge, the outermost circle is that of individual information which includes any data or category which can be attached to a person. For this concentric circle, the individual need not be personally known. Moreover, an individual does not need to be aware of the data linked to her. The next circle consists of private information that is not automatically available and only revealed under compelled disclosure enforced by law. Each individual controls the identity knowledge that he or she regards as sensitive information, selectively revealing this information to people they trust and feel close to. Unique and core identifications create a unique identity that is attached to an individual, either jointly or individually. Traditionally, unique identity tended to be synonymous with a core identity based on biological ancestry.

Figure 3 - Marx' model of identity knowledge



Research findings of a UK-based survey into public perceptions around privacy and information sharing show that participants most frequently nominate the following types of information as 'personal information': financial information (21 percent), address details (20 percent), health information (17 percent), name (16 percent), date of birth (15 percent), banking or credit card details (12 percent), and tax records (9 percent). Furthermore, participants indicated health records (82 percent) and income and

tax records (74 percent), followed by address, criminal records, and information about dependants (61 percent each), as more private types of personal information related to themselves (MORI, 2003).

In emerging e-government service environments, new personal identifiers can be introduced and used, such as a username, password, email address, click behaviour, or voiceprint (Lips, 2008; 2009a). These digitised forms of identity information can be used instead, besides, or in combination with personal identifiers commonly used in 'real world' citizen - government relationships (Greenwood, 2007; OECD 2009). Several scholars argue that, now that people increasingly are operating in digital environments, individuals have a growing amount of personal identifiers available to identify themselves in relationship with others (e.g. Clarke, 1994; Pfitzmann, 2007). Individuals prefer to keep some of these personal identifiers separate to protect their privacy, and others they prefer to link or have linked. This is also reflected in the ways in which separate government organisations define, verify, and manage citizens' personal information differently, and is balanced against the government's need to manage access to public services.

11. What is considered sensitive personal information varies with context and in relationships

What is considered sensitive personal information varies with context and in relationships: information appropriate in the context of one relationship may not be appropriate in another (Moore, 1984; Nissenbaum, 2010; Schoeman, 1984; Wacks, 1989). For example, an individual usually considers her medical information as more sensitive information than address information (Nissenbaum, 2010; Wacks, 1989); however, exchanging medical information with your GP usually is considered less sensitive than exchanging that information with your employer.

In a 2008 UK-based study, when asked which types of personal information they would be happy to have shared across government departments rather than to re-present the information during different service interactions, research participants were most happy to supply their date of birth (73 percent); educational qualifications (70 percent); and criminal records (67 percent). Respondents were unhappy to supply their bank account details (74 percent) and information about their savings and pensions (63 percent) (Institute for Insight in the Public Services, 2008).

6 *et al.,* (1998) confirm the perception that some types of personal information are more sensitive than others. In the UK, with regard to the handling of personal information, a large majority of the general public trusts family doctors, the National Health Service (NHS), and banks. Within the UK public sector, the UK tax administration and the police are less trusted than the NHS. 6 *et al*. (1998) attempted to understand more about why some organisations are more trusted with the handling of personal information: past experience of reliable performance and good reputation built up from the experience of others, are the reasons most likely to convince people to place high levels of trust in organisations to handle their personal information. The 1998 UK survey findings show that the best predictors of placing high levels of trust in an organisation's handling of personal information are: believing information to be kept securely; believing staff to be reliable with information; believing that the organisation is law-abiding, using information only for the purposes notified and personalising services (6, *et al*., 1998).

12. Individuals' privacy preferences exhibit finely tuned tendencies to disclose, share, and withhold personal information, depending on context, relationship, and type of information

An empirical study into privacy and information sharing behaviour shows that people's privacy preferences do not reflect a simple desire to control and withhold personal information, but rather exhibit shifting and finely tuned tendencies to share and withhold personal information, depending on the context of information sharing, recipients of their personal information, and the sensitivity of the information (Institute for Insight in the Public Services, 2008; Olson, Grudin, & Horvitz, 2005: in: Nissenbaum 2010, p.151).

Similarly, the results of a 2006 pan-European survey into citizens' attitudes and behaviours regarding electronic identity (eID) show that context is a powerful variable in understanding and explaining the disclosure and management of personal information by individuals (Halperin & Backhouse, 2008). The study findings demonstrate some convergence between European countries on high risk perceptions towards personal data management, global mistrust towards institutions to manage personal information, and the reluctance of individuals to use eID systems just after their launch (Lusoli & Miltgen, 2009, p. 59).

3.3.5.2 Cross-agency information sharing

13. Cross-agency collaboration is not easy, and takes time and additional effort by individuals and agencies involved. The more the clients' needs are interrelated and need to be addressed by multiple agencies, the more government agencies need to collaborate to address their information deficiencies

Collaboration efforts of government agencies can be viewed on a continuum of degrees of joined-up government, ranging from informal ad-hoc arrangements and information exchanges, to formalised collaborative initiatives on integrated service delivery (Eppel, *et al*., 2008). There is no right answer to the question what is the appropriate level of joining-up (6, 2004). Cross-agency collaboration is not easy, and takes time and additional effort by individuals and agencies involved (Lips, *et al*., 2009c). However, when the issues being dealt with are complex, fragmented and multi-causal, then it is more likely that no one agency has sufficient information or resources to address the issues alone (Conklin, 2006; Ritter & Webber, 1973). A general rule is that the complexity of the public management response needs to match the complexity of the problem. That is, the more the clients' needs are interrelated and need to be addressed by multiple agencies, the more government agencies need to move towards the collaborative end of the continuum to address their information and resource deficiencies (Bryson *et al*., 2006; Klijn, 1997).

A widely acknowledged critical factor for successful cross-agency collaboration is trust (Lips, *et al*., 2009c; Rommel & Christiaens, 2009). High trust not only results in a deeper form of collaborative behaviour between agencies, it also eases the need for control. This in turn reduces transaction costs and the need for formal contracting (Das & Teng, 2001; Ring & Van der Ven, 1992). Agencies that trust each other, engage in joint problem-solving, joint action, and increased information-sharing (Dyer &

Chu, 2003; Edelenbos & Klijn, 2007; Muthusamy & White, 2005).These agencies especially share tacit information, but also strategically important information and competencies allowing partner organisations to learn (Lips, *et al*., 2009c).

14. International research findings demonstrate that there are many cases where a citizen's personal information is still not shared when it should be, or where it is shared when it should not be.

Increasingly, improving cross-agency information sharing to enhance the effectiveness of public service provision is at the heart of public management reform efforts (6, et al., 2005; Varney, 2006). Often, these reform efforts are further supported by the introduction of new Information and Communication Technology (ICT) applications, systems, or infrastructures (e.g. Gil-Garcia, *et al*., 2007). However, with limited empirical research into cross-agency information sharing thus far, available research findings indicate that there are many cases where information is still not shared when it should be, or where it is shared when it should not be (Bellamy, *et al*., 2008, p. 737). Furthermore, recent societal 'crises' involving cross-agency collaborations, such as Hurricane Katrina in the USA or the Victoria Climbie murder case in the UK, have opened up public debate about the information sharing failings of government agencies. This has led to substantial changes to existing institutional arrangements, such as the creation of new legislation, changes to governance structures and leadership of government agencies, and the introduction of new information systems (e.g. Bertot & Jaeger, 2008; Peckover, *et al*.,2008; Wetmore, 2007).

One of the few available empirical research projects on cross-agency collaboration and information sharing looked at eight multi-agency arrangements in the UK, situated within policy domains of integrated health and social care, crime reduction, and public protection (6, *et al*., 2005; Bellamy *et al*., 2007). In the UK, increased sharing of clients' personal information has been acknowledged as critically important to cross-government collaborative approaches in the wider social policy domain, especially in such areas as child protection, crime reduction, health and social care, offender management, youth services, domestic violence and substance abuse. In all these fields, UK Central Government has promoted the increased sharing of client information among local agencies by the publication of detailed national guidance notes, the introduction of model information-sharing protocols, and the introduction of centralised information systems including a national violent and sex offenders database, a national information-sharing and assessment tool for integrated children's services, and a national police intelligence system (Bellamy, *et al*., 2008). This effort towards increased information sharing and the availability of centralised, integrated datasets has been strongly pushed by political attention to a number of high profile media cases where the lack of shared information led to disastrous social outcomes including the deaths of long-term abused children, rapes by sex offenders known to the police, and murders by violent offenders living in the community (e.g. Bellamy, *et al*., 2008; Taylor, *et al*., 2006).

In general, the research findings show that, with strong political pressure and detailed prescription to increase information sharing, information sharing practice is patchy, even within the same organisation (6, *et al*., 2005; Bellamy, *et al*., 2007). Furthermore, consistency of information sharing is dependent on how discretion is exercised in individual cases. As information sharing decisions need to be taken by

individual front-line staff members within detailed national information-sharing guidance frameworks and on a case-by-case basis, professionals face continual dilemmas between the risk of 'false negative' error judgments (i.e. when no action is taken, but where it turns out later that it should have been taken) and the risk of 'false positive' judgments (i.e. where action is taken, although it turns out later that the risk was lower than would justify it) (6, *et al*., 2005). Generally, the people involved in these cross-agency arrangements show greater confidence that confidentiality would be respected appropriately, than that information would be shared appropriately. For instance, informal practices were used to address gaps, deal with inconsistencies, and reduce bureaucratic transaction costs associated with existing legislation and other forms of formal regulation (Bellamy, *et al*., 2008, p. 753). The overall conclusion of the research is that both deficits in social integration of public officials in cross-agency arrangements and deficits in formal regulation are significant in inhibiting the development of consistent and appropriate information-sharing practices across the UK social policy sector (6, *et al*., 2005; Bellamy, *et al*., 2008; 2007).

15. Research shows significant barriers to cross-agency information sharing in organisational, political and legal, and technical domains

Generally, available literature point at significant barriers to cross-agency information sharing in organisational, political and legal, and technical domains. Based on an extensive literature review Gil-Garcia *et al.* (2007, pp. 123-124) provide the following examples under each category:

Organisational barriers: significant barriers can be located both at the meso-level of the organisation and at the micro-level of individual employees. At the meso-level, barriers are due to explicit and implicit differences among the organisations participating in a cross-agency collaborative arrangement and include misaligned organisational missions, conflicting organisational priorities, diversity in organisational cultures, lack of funding, limited access to implementation models or guidelines, and a lengthy time frame for the manifestation of organisational benefits. At the micro-level, barriers include resistance to change, different individual agendas and goals, misinterpretation of shared information, and misuse of shared information.

Political and legal barriers: important barriers include the lack of executive and legislative support, restrictive laws and regulations (e.g. civil service regulations), and the requirement to assure citizens' privacy and confidentiality.

Technical barriers: barriers include incompatibility of hardware or software, mismatched data structures, incompatible database designs, incongruous data and information distribution channels, and conflicting data definitions and different terminology.

16. International research suggests a lack of confidence in corporate governance of organisations responsible for collecting, storing and sharing significant amounts of personal information

Backhouse and Halperin (2007) report on the social aspects associated with sharing data, especially personal information, based on a survey of 1906 citizens in 23 EU countries. Overall, the findings point

to a negative perception of ID authorities by EU citizens – they are seriously critical of the competence of ID authorities, and dubious about authorities' ability to handle personal data with appropriate care. The most negative attitudes are found in the UK and Ireland.

3.3.5.3 Implications of information sharing

17. *Available literature points at two different perspectives on the management of citizen identity information in e-government service environments: a 'Surveillance State' perspective and a 'Service State' perspective (see Figure 4). UK-based research suggests that attributes of both perspectives can be observed in e-government service environments when looking at the actual use of citizen identity information.*

With the introduction of new e-government service environments including new ways of sharing and managing citizen identity information, governments not only perceive opportunities to enable the modernization of their organization, they also see advantages of transforming their service provision to the citizen (Varney, 2006). A well thought-out approach to the sharing and management of citizen identity information is expected to bring a wide range of possible benefits to government agencies, including increased efficiency and reduced costs; improved effectiveness in public service provision; innovation and joined-up service provision; enhanced information security and privacy; improved customer convenience and access to public services; improved monitoring to ensure compliance, equitable enforcement, exclusion of unwanted people and activities, or enhanced personal and public protection; and a step increase in the provision of e-government services by enhancing trust and confidence in online interactions with citizens (Lips *et al*., 2009b; OECD 2009).

The introduction of new digital ways of sharing and managing citizen identity information may not only bring about benefits to government agencies however; they are also expected to lead to significant changes in the relationship between the citizen and the State (House of Lords 2009; London School of Economics, 2005). Advances in technological capability embodied in these new digital ways of sharing and managing citizen identity information may bring about substantial informational imbalances in citizen – government relationships to the disadvantage of the citizen (Crossman, 2007; London School of Economics, 2005).

In general, the following changes to informational relationships are observed as a result of introducing new ways of sharing and managing citizen identity information in e-government service environments (Lips, *et al*., 2009b; Camp, 2003; Marx, 2004):

- information can flow freely and in ways that are difficult to trace, compared to information in face-to-face and paper-based transactions within the confines of a physical locale and relatively closed networks;
- information can be copied and stored at almost no expense;
- an increased merging of previously compartmentalized identity information on the citizen;
- transactions become information dependent, with current identification systems relying on the confirmation of an individual's information;
- transactional histories become more detailed and easily available to many;

- trust depends on transactional history reports rather than on personal recognition; and
- an increased blurring of lines between public and private places makes citizen identity information more publicly available.

Based on these informational trends, several scholars point at fundamental changes which may happen to informational relationships between the citizen and the state as a result of the introduction and use of new digital forms of citizen identity management (IDM) (Lips *et al.* 2009b). Interestingly however, scholars seem to have almost opposite views on the direction and outcomes of these fundamental changes (Taylor *et al*, 2009). We describe each of these opposite views, which we refer to as a 'Surveillance State perspective' and a 'Service State perspective' respectively, more in detail below (for further details, see Lips *et al*. 2009b).

Surveillance State perspective

Several scholars perceive fundamental changes happening as a result of a developing surveillance society in which government uses digital IDM systems as surveillance systems with a substantial impact on democratic citizen rights (e.g. London School of Economics, 2005; Murakami-Wood, *et al*., 2006); They point out that the introduction and use of newly available IDM systems is leading to substantial information imbalances in citizen – government relationships (e.g. London School of Economics, 2005; Lyon, 2001; Murakami-Wood, *et al*., 2006). Digital IDM systems are acknowledged as 'surveillance systems' which can monitor individuals' behaviour as well as collect and process individuals' identity information. Generally, surveillance is defined as "any collection and processing of personal data, for the purposes of influencing or managing those whose data have been garnered" (Lyon, 2001, p. 2).

Many scholars signal an emerging trend of surveillance 'creeping' into all aspects of society with profound implications for democratic citizen rights (e.g. Lyon, 2006; Ogura, 2006). For instance, a study produced by the academic Surveillance Studies Network points at developments in the UK where individuals' daily lives are enveloped by massive surveillance systems. Available ICTs, such as mobile phones, CCTV Cameras, Satellites, RFID tags, Internet cookies, and email traffic, offer unprecedented automated ways to gather and process personal information of individuals: "where we find purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence or protection, we are looking at surveillance" (Murakami-Wood, *et al*., 2006, p. 4). As an outcome of rationalization practice in organizations, the use of digital IDM systems can support the modern state in its efforts to enhance speed, control and coordination (*ibid*.)

In general, several scholars point out that personal and group data captured by surveillance systems can be used to classify people and populations according to varying criteria, to determine who should be targeted for special treatment, suspicion, eligibility, inclusion, or access, for example (Lyon, 2003; Murakami-Wood, *et al*., 2006). Consequently, surveillance systems are discriminatory technologies as they sieve and "socially sort" for the purpose of assessment thus affecting people's life chances (Lyon, 2003, p. 20). However, surveillance does not proliferate just because of the *availability* of new IDM systems: the development of surveillance is determined by the *use* of these IDM means by government or other organisations (Lyon, 2001, p. 74).

Service State perspective

Many scholars point at a strong alignment between opportunities offered by newly available ICTs and a New Public Management (NPM) style of reform (e.g. Bellamy & Taylor, 1998; Filipe Araujo, 2001; Hood, 1991; Margetts, 2003). New digital ways of sharing and managing citizen identity can enable innovation in public service provision to citizens, offering governments the opportunity to break down 'vertical' government silos and deliver integrated, more effective public services which meet the holistic needs of the citizen (Dunleavy, *et al*., 2006). In general, the quest for better coordinated, 'joined up' or more integrated forms of government have led to growing pressure for the sharing of citizens' personal information among public service agencies (6, *et al*., 2005; Bellamy, *et al*., 2007). Due to newly available pervasive information-handling opportunities which can offer a response to emerging public sector problems resulting from NPM reforms, Dunleavy *et al.* (2006) point at the emergence of a new public management reform model of 'Digital Era Governance'. This Digital Era Governance Model can be characterized under the following three themes (Dunleavy, *et al*., 2006, pp. 227-242):

- Reintegration: ICTs will put back together many of the functions and expertise clusters that NPM separated into single-function organizational units. Examples are the use of digital IDM systems to facilitate joined up government or to re-strengthen central processes in order to reduce duplication across government;
- Needs-based holism: ICTs will simplify and change the entire relationship between agencies and their clients, moving away from the NPM focus on business process management and towards a citizen- or needs-based foundation for organization. Examples are IDM-enabled public service reorganizations around a single client group or ask-once processes supported by reusing already collected citizen information;
- Digitization changes: electronic channels become the central feature of administrative and business processes. Examples are new forms of automated processes where no human intervention is needed in an administrative operation, such as electronic monitoring of customers (e.g. patients) or increasing transparency and offering citizens to track and self-monitor the processing of their service applications.

These two emerging perspectives on the Surveillance State and the Service State are summarized in Figure 4.

Empirical research into the use of digital ways of sharing and managing citizen identity information in a variety of e-government service environments in the UK, shows that no particular perspective is dominant: characteristics of both perspectives are visible in these UK case studies simultaneously and in parallel, albeit within the legal restrictions of UK data protection legislation and not violating a citizen's privacy rights or individual freedom so far (Lips, *et al*., 2009b). Consequently, depending on the actual use of citizen identity information, the same informational options can lead to outcomes which can be classified under a Surveillance State perspective or a Service State perspective (*ibid*). Moreover, there can be a distinction between information sharing intentions of agencies and perceptions of e-government users on the use of personal information in public service provision: for example, although agencies are operating under a Service Transformation paradigm, the perception of e-government users can be the implementation of a Surveillance paradigm (*ibid*).

Figure 4 - Surveillance State Perspective vs. Service State Perspective on managing citizen ID data

Attribute	Surveillance State perspective Meaning	Service State perspective Meaning
Increased and systematic use of digital citizen IDM systems	Surveillance systems leading to rationalization and control	Public service support systems leading to service transformation
IDM objective	Risk management, 'knowing the unknown'; increased efficiency	Targeted public service provision; CRM; increased effectiveness
Purposeful attention to citizen identity information	Surveillance	Better public service provision
Increased information-sharing	Increased analysis; matching and merging of citizen identity information; profiling	Reduced duplication and fragmentation; joined-up government; integrated public service provision
Client focus	Monitoring; segmentation of service users; social sorting	Holistic needs-based service provision; personalization; citizen-centric government
Implications for citizen-government relationships	Increasing information asymmetries; eroding trust	Decreasing information asymmetries; increasing trust
Citizen rights' implications	Violation of privacy and individual freedom rights	Improved access to public services; open government, transparency

Source: Lips *et al*. 2009b, p843

3.3.6 Informational privacy

18. Privacy is a multifaceted, ambiguous notion which means many things to many people.

Privacy is a multifaceted, ambiguous notion which means many things to many people (6, 1998; Buchanan, *et al*., 2007; Nissenbaum, 2010). Privacy is also culture and context-specific, with people from different cultures attaching different meanings to this concept (Moore, 1984): for example, people from Asian countries usually have a different perception of privacy compared to people from New Zealand.

Nissenbaum points at a wide-ranging set of theoretical perspectives about privacy and suggests a scheme with three dimensions of difference across the set of privacy theories: 1) normative accounts vs. descriptive ones; 2) definitions given in terms of access from those given in terms of control; and 3) accounts that locate the source of privacy's prescriptive power in its capacity to promote other important values, from accounts that locate its prescriptive power in the capacity to protect a specific, private realm from access by others (Nissenbaum, 2010, p. 67). In order to overcome problems around seemingly incommensurable differences between normative and descriptive accounts of privacy (e.g. the assumption of privacy as an absolute right), Gavison (1980) proposes a neutral conception of

privacy. In her view, a neutral conception of privacy would have the advantage of being able to talk about increased or decreased levels of privacy, without any normative claim of this particular impact on privacy is good or bad.

The highly complex nature of privacy has resulted in alternative ways of defining it through various dimensions, including the dimension of *informational privacy* (e.g. Burgoon, *et al*., 1989; DeCew, 1997). According to Malhotra *et al*. (2004), informational privacy refers to the claims of individuals or groups to determine for themselves when, how, and to what extent information about them is communicated to others (Malhotra, *et al*., 2004).

Based on research findings from a large survey in the UK, 6 *et al*. (1998) note the conventional recognition of four groups of attitudes to privacy in the population:

1. ***privacy fatalists:*** who believe that there is little that they or anyone else can do to ensure proper use of personal information;
2. ***privacy unconcerned:*** who are content that any person or organisation may collect information about them and see only benefits rather than risks to this;
3. ***privacy fundamentalists:*** who are reluctant to provide personal information and believe that there are high risks that it will be used unfairly to disadvantage them; and
4. ***privacy pragmatists:*** who are prepared to provide personal information to organisations in return for enhancements of service or other benefits.

6 *et al*. (1998, p. 12) conclude that although pragmatists were the largest group in the 1998 UK-based survey, it could be that most people do not have a fixed position within these four groups but a repertoire from which individual decisions are made in each context and case. For example, 6 *et al*. (1998) observed that, with prompting, most people are aware of data protection laws but many have fears about the costs, difficulty, and efficacy of using these enforcement strategies.

Viseu *et al*. (2004) partly explain the ambiguous nature of privacy by the fact that informational privacy points itself in the direction of the individual rather than the social. The individual nature of privacy is revealed for instance in comments such as 'nothing to hide'. As a result, a short-term individual perspective is dominant: the gains of releasing personal information over the Internet are immediately achieved, while the societal risks to personal information use are abstract and distant. Individual action towards a privacy ideal is neither well defined nor perceived as attainable. Privacy statements on websites are largely generic and go unread. They conclude that online privacy is best understood as an environment that simultaneously contains and is contained in people's activities.

19. The meaning of informational privacy is changing under the possibilities opened up by new ICT

The meaning of privacy is changing under the possibilities opened up by new ICTs (6, 1998). In general, ICT-enabled changes to informational relationships as described earlier under theoretical assumption 17, raise several fundamental questions and dilemmas for governments in developing e-government service relationships with the citizen. For example, an individual’s ability to remain unidentified has

declined significantly in IDM enabled e-government service relationships, causing deep concerns about an individual's informational privacy protection for instance (FIDIS, 2006). At the same time however an increased freedom of choice can be observed for individuals to represent themselves, such as the use of different types of pseudonyms (e.g. email-address, a fake name) in interactions with others, including government agencies. A related example is new opportunities to access, copy and abuse someone else's informational details presented in e-government service transactions in order to get certain benefits.

Another example is the use of shared, matched or merged identity information on the citizen in order to provide new 'personalised' or integrated public services to individuals (Dunleavy, *et al*., 2006; Lips, *et al*., 2006). With these new opportunities for public service provision, an important dilemma for governments is how to manage a potential tension between policy goals of better coordinated or integrated public services to individuals in a customer-focused way, requiring more extensive data sharing, whilst protecting fundamental citizen rights like an individual's privacy (6, *et al*., 2005; Bellamy, 6, & Raab, 2005). As new digital identification systems offer possibilities to make use of citizens' identity information in new ways, including for tasks that are far removed from the purposes for which personal data were originally collected, they may cause conflict with data protection regulations (6, *et al*., 2005; Bellamy, *et al*., 2005; FIDIS, 2006; Halperin & Backhouse, 2008).

A further example is the possibility that collected identity information on the individual can be securely stored in a government database which can then be accessed by government officials or third party representatives to make copies from, match with other available data, or run secondary data analysis (Birch, 2007). Put differently, a situation which usually is perceived as enhanced information security compared to identity information stored in paper based files for instance, actually may lead to new security risks. A related example would be the availability of a back-up copy of a secure government database, which could be accessed by public servants or others and, for instance when stored on a memory stick, lost or stolen.

Examples such as these suggest that new ICT-facilitated public service relationships between government and citizens require a deep reconsideration of mutual rights and responsibilities around informational privacy and the sharing of personal information (Lips, *et al*., 2009b; Taylor, *et al*., 2007). Moreover, the introduction and use of ICTs in e-government service relationships have radically altered the terms under which others (e.g. government agencies, private sector organisations, individuals) have access to the individual and to information about the individual in what are traditionally understood as private and public domains (Nissenbaum, 2010). According to 6 *et al*. (1998), as privacy no longer means preventing organisations and other people from knowing about us, it needs to be founded on securing organisations' commitment to principles about what shall and shall not be done with personal data. In their view, privacy cannot be an absolute right but is best understood as protection against certain kinds of risks, such as risks of injustice through unfair interventions for instance, risks of loss of control of personal information, and risks of indignity through exposure and embarrassment.

20. Concerns expressed about privacy do not necessarily translate to online behaviour

Several scholars observe a difference between peoples' expressed concerns about privacy and their actual behaviour (e.g. Nissenbaum 2010). For instance, in 2000, a Pew Internet Project study on trust and privacy online surveyed more than 2,000 American Internet users (Fox, 2000). They found respondents are concerned about their privacy in the online environment, despite only a few experiencing any significantly detrimental breaches of their privacy and the majority undertaking trusting and intimate activities online. Further, respondents desired privacy protections within the online environment but knew little about how to achieve this or how their information was used.

Further evidence for this assumption is found in the findings of an ethnographic research project. As evidenced empirically in their study of peoples' everyday Internet use in a middle class neighbourhood of a Canadian city, Viseu *et al*. (2004) point at a significant discrepancy between concerns about privacy, privacy principles, and an individual's privacy practices. They found that location, life stories, and experiences affected peoples' perceptions of privacy: for example, research participants reported their concern about their privacy when conducting financial transactions on a computer they do not own; their trust in Canadian online transactions but not Brazilian ones; and their restriction of online transactions to a place of work and not their home. Secondly, the researchers found a dynamic interaction between the goal of an individual's online activity, his or her perception of the medium, and the strategies used in his/her self-presentation.

In general, Viseu *et al*. (2004) found Internet users passive in their privacy protection strategies, with only one participant using privacy enhancing technologies for instance. The most frequently observed attitudes to privacy were resignation, dismissal, and annoyance. Overall, Viseu *et al*. (2004) conclude that privacy had minimal impact in shaping their participants' online activities.

21. There is a tension between privacy and the use of personal information to achieve more convenient public services for citizens

Research demonstrates that, in being able to choose between service channels including new ICT-enabled service environments in which more personal information is collected on the customer, people choose the options that offer convenience, speedy passage, financial savings, connectivity, or safety, rather than those that offer privacy. Furthermore, only 20 percent of people claim to read privacy policies most of the time and no more than 7 percent complain about these policies (Nissenbaum, 2010, p. 105). For example, an Australia-based survey found that individuals consider privacy risks as a trade off for the convenience of the online service environment (Australian Communications and Media Authority, 2009).

Further evidence can be found from research in which real life scenarios about the use of personal information are presented to individuals. When realistic cross-government information sharing scenarios were presented as part of a UK-based research activity, participants were less likely to be concerned about the privacy implications of information sharing practices: approximately 45 to 50 percent of participants reported they would not be concerned at all about this kind of sharing, with the lowest concern among participants when the scenario included a benefit to the individual (MORI, 2003).

A similar result was found by another UK-based study of public attitudes to privacy and cross-government data sharing (Institute for Insight in the Public Services, 2008). In this study, participants responded negatively to general notions of data sharing across government but less so to real life scenarios where data sharing could benefit the service provider and recipient/s of that service.

22. There is a tension between privacy and the use of personal information to support public safety

Based on the notion of a democratic society consisting of a collection of relatively autonomous individuals, privacy can be in conflict with social and community values (Bennett & Raab, 2003). Several scholars point at conflicts between privacy values and security or public safety values, particular in the wake of the September 11, 2001, attacks on the World Trade Centre (e.g. Nissenbaum, 2010; O'Harrow, 2005; Regan, 1995). For example, in the USA, law changes after this societal crisis have led to increased video surveillance of public spaces, more eavesdropping on mediated conversation, more identity checkpoints, and closer scrutiny of activities, transactions, purchases, travel and financial flows (Nissenbaum, 2010). Furthermore, a dominant perception emerged among US policy makers that an effective response to terrorist threats will require more extensive information sharing among government agencies (Roberts, 2004).

However, perceptions of the general public on the implications of increased sharing of personal information for the purpose of security may be different compared to those of policy makers. For example, in a nine-country opinion survey of peoples' views on surveillance, privacy and global information sharing, when people were asked the question "to what extent is your privacy respected by airport and customs officials when travelling by airplane?", more than 82 percent of the respondents reported feeling that their privacy is "completely", "a lot", or "somewhat" respected by airport officials (Zureik, 2008). This is a remarkable finding, as substantial identification processes involving the collection of personal data (e.g. X-raying, body checks) are used at most international airports nowadays (Nissenbaum, 2010).

23. Available literature points at possibilities of 'function creep' or 'mission creep'

Several scholars point at the possibility of 'function creep' – the use of collected, digital personal data for another purpose then originally intended (Bennett & Raab, 2003). Koops *et al*. (2007) particularly observe function creep happening as a result of the increased use of common identifiers, such as unique numbers, that connect data repositories across government.

Clarke (1988) introduced the notion of 'dataveillance' – the systematic use of information itself in the investigation or monitoring of the actions or communications of one or more individuals. Nissenbaum (2010) points at the fact that, in many cases, dataveillance can be seen as a form of function creep: dataveillance often is not the direct aim but an unintended consequence of some other goal for which a given system was originally designed. Examples are credit card payment statements which reveal an individual's whereabouts, or telephone bills intended for the settling of payments, which provide information about an individual's conversations (Nissenbaum, 2010, p. 24).

Gellman introduces an alternative form of 'function creep' which he calls 'mission creep': the use of a database facility for a different purpose or functionality (Gellman, 2004, p. 500). Using the example of the history of credit reporting in the USA, Gellman points at the development of database derivative activities and the risks involved of these activities. For instance, any database will contain errors which will have significant consequences for individuals who use public services facilitated through database derivative activities.

3.3.7 Trust in the e-service environment: information security

24. Robust identity management is identified as an enabler of trust in e-government service environments

The management of citizen identity information or 'Identity Management' (IDM) can be a critical enabler for the uptake of e-government services (OECD 2009). For instance, 6 *et al*. (1998, p. 13) point out that the best predictors of placing high levels of trust in an organisation's handling of personal information are:

1. believing information to be kept securely;
2. believing the staff to be reliable with information;
3. believing that the organisation is law-abiding;
4. using information only for the purposes notified; and
5. personalising services

Identity Management (IDM) can be defined as the set of rules, procedures, and technical components that implement an organisation's policy related to the establishment, use, and exchange of digital identity information for the purpose of accessing services or resources (Birch, 2007; OECD 2009). Robust IDM is expected to bring a wide range of possible benefits to government agencies, including improved efficiency and effectiveness in public service provision; innovation and joined-up service provision; enhanced privacy and security of citizen identity information; improved customer convenience and access to public services; and a step increase in the provision of e-government services by enhancing trust and confidence in online interactions with citizens (Lips, *et al*., 2009a; OECD 2009).

An important element of robust IDM is the security of IDM systems. OECD (2009) note the following challenges in ensuring effective security: confidence by users of availability, access, and reliability of digitised personal information and transfer by those with legitimate authority and purpose; minimisation of disruption or corruption; the impact of architecture, design, and technology choices on information security and privacy; auditing and controls on sensitive personal data; and developing processes and procedures to address the possibility of data breaches.

Crompton points at the trust challenges that have arisen from IDM solutions which have been mainly focused on the needs and interests of the organisation, instead of on the interests of individual users. To achieve mutual trust in the management of citizen identity information in e-government service relationships, he suggests that organisations must consider the following dynamic and interdependent factors from the viewpoint of the individual (Crompton, 2008, p. 6):

- Fair risk allocation: ensuring that individuals understand the risks around the management of personal data and are confident that they are fairly allocated to the party most able to bear them;
- Control: ensuring that individuals have the control they want over how personal information is demanded, collected and stored, or if that is not possible or wanted, they understand the organisation and how it will handle the information;
- Accountability: ensuring that the organisation is accountable and transparent about how it will handle personal information and take appropriate responsibility for dealing with the impact of failure on the individual including having a good safety net.

25. Dominant barriers to online public service consumption relate to an individual's perception of risks associated with the online environment.

Peoples' perceptions of risks associated with the online environment influence customer expectations and satisfaction with online public services (National Research Unit, 2009; Rotchanakitumnuai, 2008). Perceptions of risk or the uncertainty regarding possible negative consequences of accessing a service are typically concerned with customer anxiety about the security and privacy of the online environment (Rotchanakitumnuai, 2008). Other risks for the online service user include the threat of financial loss, poor performance, and reduced convenience. More specifically to public service consumption in the tax administration environment, barriers to using online services include the customer's comfort, reliance, and trust with other service channels; not being technically confident or knowledgeable; not having access to appropriate technology; and not trusting the online filing system (Kelly & Hopkins-Burns, 2010).

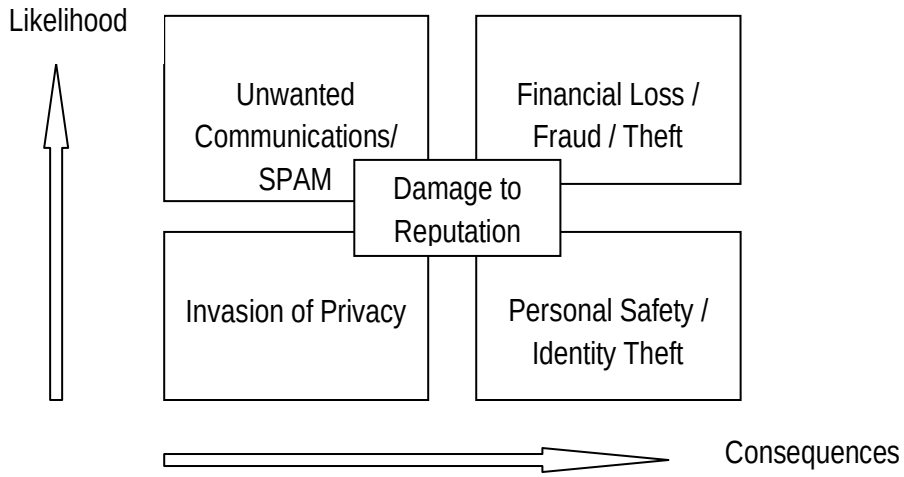
Research findings of a 2009 Australia-based study into attitudes towards the use of personal information online show that participants perceived the following risks as inherent to disclosing personal information online: risks to personal safety and wellbeing; identity theft; financial loss; reputational damage; invasion of privacy or access to personal information without permission; and exposure to spam and other unwanted communications (Australisan Communications and Media Authority 2009). Research participants assessed the risk of disclosing personal information online by weighing the perceived likelihood and severity of the consequences (see Figure 5 below).

26. Threats to the security of personal information can come from human fallibility (e.g. human errors), technological fallibility (e.g. ICT reliability), or from the interaction between human and technological fallibility (e.g. the loss of sensitive or confidential data stored on a CD or USB stick)

The human factor often is responsible for the failure of secure information systems and threats to information security and privacy (Bennett & Raab, 2003; Lusoli, *et al*., 2009; Schneier, 2004). Schneier (2004) points out that secure information systems cannot be perceived in isolation: there is always the need to interact with users in some way, at some time, for some reason. In his view, securing the interaction between people and information systems is a huge problem for the following two reasons:

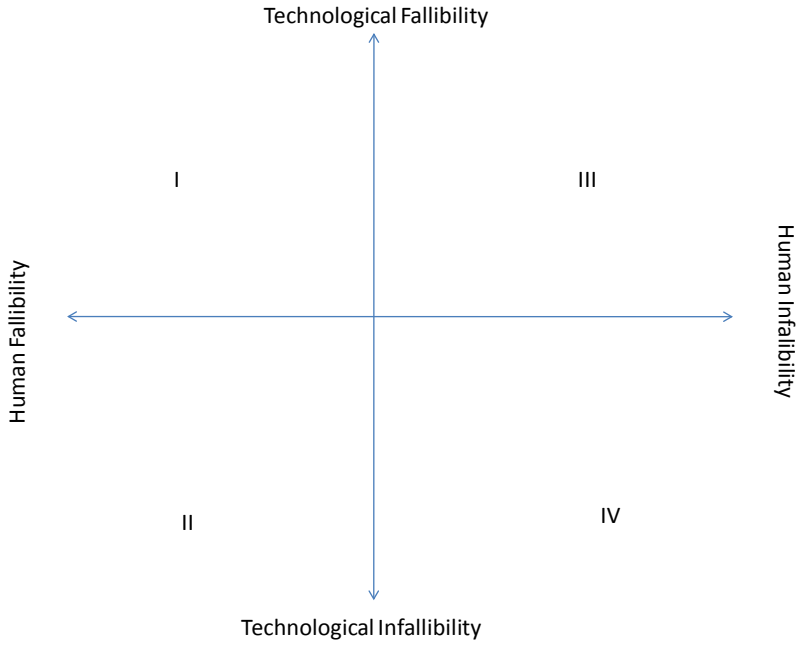
a. People do not understand the risks involved in working with information systems;
b. Moving and keeping digital information within the boundaries of a secure information system is impossible, as information never stays in such a system, but moves onto paper for instance.

Figure 5 - Perceived severity of risks associated with the use of personal information online (AMCA 2009, p. 14)



Privacy problem sources are many and complex, and are often related to a combination of human and technological factors. To explain the range of privacy problem sources, Bennet and Raab (2003) offer the following matrix with technological fallibility/infallibility on one axis and human fallibility/infallibility on the other (see Figure 6).

Figure 6 - Matrix of privacy problem sources (Bennett and Raab, 2003, p. 28)



Bennet & Raab (2003) explain that most privacy related problems tend to be seen where human fallibility combines with technological fallibility (category I problems). However even where technologies and humans combine to perform perfectly as intended, new levels of intrusiveness can be reached (category IV problems). Sometimes the quality of human performance can be high but the technologies might fail (e.g. old databases, inaccurate databases, poor processing, or malicious attacks on databases) (category III problems); One the other hand, technologies might perform as intended but humans might draw the wrong inferences or conclusions, or make mistakes while inputting data (category II problems).

Lusoli *et al*. (2009) point at the emerging issue of to what extent individuals can be held accountable for the accuracy of their personal information provided in e-government service relationships. This also applies to the handling of personal information by public sector staff members.

As an example of the fact that humans are often the weak link in the security chain, KPMG (2008) points at an increasing number of personal data loss incidents across the UK public sector: between 2005 and 2008, 1034 incidents were reported, with 404 in 2008 alone. Government organisations were responsible for 19 percent of the data loss incidents between 2007 and 2008, with the majority of incidents caused by external contractors. Portable media, such as laptops and other removable media like USB keys or CDs turned out to be highly vulnerable from an information security risk point of view.

3.3.8 Awareness

27. People have little awareness of what personal information is held by public sector agencies

Research findings of a UK-based study show that participants had little awareness of what personal information is held by government: 64 percent of participants reported they do not feel well informed. Further, when asked if they know how to determine what personal information government agencies hold about them, 4 percent of the respondents did not know; 53 percent reported they do not know what their rights regarding personal information are; and 68 percent reported they do not know how to formally complain about the way government handles their personal information. The latter situation was particularly observed for those participants with low education and income levels (MORI, 2003).

People form their opinion on risks associated with the online environment essentially through the media. In Australia, the media is the primary influence on Internet users' perception of the risk of online identity theft (Australian Communications and Media Authority, 2009). Some participants acknowledged that identity theft could also occur outside the online environment.

Compared to the influence of anecdotes on identity theft and other online risks disseminated by the media, actual experience of these online risks often is relatively limited. For example, in the USA, a study conducted by the Pew Research Centre found that just 4 percent of American Internet users have had negative experiences where inaccurate or embarrassing material about them was posted online (Madden & Smith, 2010, p. 27).

28. People operating in online environments lack crucial knowledge about privacy practices and available tools

Awareness of informational privacy risks does not necessarily translate into taking steps to protect privacy, even when there is knowledge of the risk, or knowledge and availability of the tools to lower that risk (Viseu, *et al*., 2004; Buchanan, *et al*., 2007; Madden & Smith, 2010). For instance, a 2009 Australia-based study found that, although many Australian Internet users have high levels of awareness about how to protect their personal information from being accessed inappropriately, common steps to mitigate risks are often not taken or not understood to be available (Australian Communications and Media Authority, 2009). For example, respondents had little awareness of how their personal information is collected, stored, and used when faced with accepting end-user licensing agreements to purchase software.

Buchanan *et al*. (2007) examined citizens' privacy concerns and their concerns about privacy-protecting behaviours. In their survey questionnaire the researchers focused on the general and technical protection steps Internet users may take to protect their privacy during online interactions. Their study found people with higher levels of privacy concern generally take higher levels of general precaution, but not technical precaution. Technical precaution tended to be taken by people with higher levels of technical skills without any relationship to privacy concern.

3.3.9 Experience, skills, ease of use

29. Previous experience, training and skills, and Internet access, support the uptake of e-government services. A barrier to e-government service uptake is familiarity and comfort with existing service channels

A UK-based study investigating customers' attitudes and experiences of filing tax returns online found that respondents, who are confident with computers and the Internet, generally perceive online filing as inevitable and something to be embraced; however, those respondents with little familiarity with ICTs were found to be less willing to try online filing (Her Majesty's Revenue and Customs, 2008). Familiarity and comfort with existing habits and routines of paper filing was the most important barrier to the uptake of online filing. The concern many respondents raised is that any new system would require a significant effort without offering substantial advantages (*Ibid*): those respondents who have never used online filing found it hard to imagine how the process would work in practice, and how similar it would be to the paper forms they feel familiar with. Furthermore, many customers were concerned that online services may not be fully reliable or secure. Finally, those individuals without Internet access or the skills to navigate online filing expressed strong concerns about and significant barriers to the adoption of online tax filing services (Her Majesty's Revenue and Customs, 2008).

Gil-Garcia *et al*. (2007) point at previous experience, positive training experiences, and personality as individual user characteristics associated with the uptake of e-services.

A 2000 Pew Internet and American Life Project study (Fox, 2000) found that about a quarter of Internet users have provided fake information in order to avoid providing real information online. In contrast, Viseu *et al*. (2004) found that participants did not use deception strategies; rather, they were selective about releasing personal information, and always used their real identity. Respondents' reasons for this strategy ranged from innocence and lack of experience of the online environment, to a desire for customisation and minimisation of the information flow and the need to establish trust.

In one of the few empirical studies of privacy behaviours, a controlled investigation demonstrated that when online merchants' privacy policies are made salient, consumers prefer to purchase from those with better privacy policies even if, in some instances, this means paying more for the goods (Tsai, Egelman, Cranor, & Acquisti, 2007, in: Nissenbaum 2010, p.106).

3.3.10 Transparency

30. There is a lack of transparency around ICT-enabled information aggregation and analysis in varying relationships between individuals and organisations

Cross-government information sharing has always occurred but recent and improved technology enables data-sharing to occur on a more significant level and with more speed than ever before (Camp, 2003). Available literature suggests that new ICT-enabled forms of access to government services are generating largely unseen and unrecognized customer information that often underpins the e-government service relationship (Taylor & Lips, 2008; Koops, *et al*., 2007). Furthermore, although the use of new ICT-enabled systems for the aggregation and analysis of personal information is not necessarily hidden to individuals, these systems or practices are usually not advertised nor transparent (Gandy, 1993; Lyon, 2007; Solove, 2004).

Whereas scholars like Gandy and Lyon point at the negative consequences of automated forms of information aggregation and analysis, leading, in their view, towards profiling and differential treatment or "social sorting" (discrimination based on demographic characteristics of an individual), Nissenbaum (2010) sees also positive outcomes emerging from the same informational practices, depending on the context in which these informational practices are applied. For example, Nissenbaum points at improved diagnostic tools for individual and community health, assisting physicians in making sense of puzzling symptoms and enabling public health officials to detect patterns of illness pointing to environmental hazards, compared to information aggregation and analysis practices by commercial entities like ChoicePoint, who offers citizen identity verification services to US government agencies, including Social Security number verification, and has publicly admitted to have sold the personal records of more than 163,000 individuals to identity thieves (Nissenbaum, 2010).

31. Transparency enhances the protection and security of citizen identity information by supporting citizens' control over their personal information

Several authors see increasing transparency to the citizen as a way to better protect citizen identity information, improve citizen control over their own personal data, and enhance citizen trust (e.g. OECD 2008; Thomas & Walport 2008; Lusoli *et al*., 2009). More specifically, increased transparency could be achieved by the following (Lusoli, *et al*., 2009; OECD, 2008; Thomas & Walport, 2008):

- Allowing citizens to easily see and understand who uses the data, what the information may be used for, and who will have access to the data;
- Allowing citizens to give informed consent to the use of their personal information;
- Allowing citizens to see what data other parties have on file concerning them and the opportunity to contest those records;
- Implementation of fair information practices by organisations.

Furthermore, available literature points at specific measures government can take to increase public confidence in the security of information collected, stored, and shared by government agencies. The following items have been identified in the literature as likely to increase public confidence in the security of personal information collected, stored and shared by government and non-government organisations. Transparency in citizen – government information relationships is a key element of each of these solutions (Thomas & Walport, 2008):

a. the use of a prominently displayed privacy policy, available in print and online, which states what information organisations hold, why they hold it, how they use it, who can access it, with whom they share it, and for how long they retain it;
b. public bodies should publish and maintain details of their data-sharing practices and schemes, and should record their commitment to do this within the schemes they are required to publish under legislation;
c. organisation should publish and regularly update a list of those organisations with which they share, exchange, or to which they sell, personal information, including 'selected third parties';
d. organisations should use clear language when asking people to opt in or out of agreements to share their personal information;
e. organisations should do all that they can (including better use of technology) to enable people to inspect, correct and update their own information – whether online or otherwise.

These suggestions for increased transparency are based on research findings like those observed in a UK-based study into public perceptions of data sharing and privacy. Participants mentioned the following reasons for their concerns with cross-agency information sharing: the lack of control over their personal information (25 percent); that they did not know who had access to their personal information (20 percent); that they did not know what information was held about them (18 percent) or what was being done to it (18 percent); information sharing without their permission (16 percent); government sharing of their personal information was an invasion of their privacy (2 percent); the security of their personal information (1 percent); paying more taxes (1 percent); and the fear of losing a benefit (1 percent) MORI (2003).

3.4 Summary of the defined theoretical assumptions under the analytical themes

An overview of the theoretical assumptions, including the literature where they can be found, is provided below:

Individuals' acceptance and use of the Internet

1. Scholars generally make a distinction between Internet users, non-users, and ex-users. Dutton, W. H., Helsper, E. J., & Gerber, M. M. 2009; Smith, *et al*., 2010; Norris, P. 2001; OECD, 2001; Mossberger, *et al*., 2008; Van Dijk, 2005
2. E-Government researchers commonly distinguish between e-Government service use categories of 1) Looking up public sector information online; 2) Interacting with government agencies online; and 3) doing transactions with government agencies online. Layne & Lee, 2001; Andersen & Hendriksen 2006; Smith, *et al*., 2010; State Services Commission, 2010; Millard, 2006

Channel Choice

3. Channel choice is driven by the perceived value associated with the channel. Broekhuizen & Jager, 2003; Her Majesty's Revenue and Customs, 2008; Rotchanakitumnuai, 2008; Torgler, 2007; Kelly & Hopkins-Burns, 2010; Millard, 2006; State Services Commission, 2010
4. Online channel adoption is influenced by trust. Camp, 2003; Connolly & Bannister, 2007; National Research Unit, 2009; Backhouse & Halperin, 2006
5. Individuals often use multiple channels to access public services. State Services Commission, 2010; National Research Unit, 2009

Trust in government and/or the service providing organisation

6. Citizens' trust in the public service contributes to the broader concept of trust in government. Citizens' trust in government is fluctuating within and across countries, as well as over time. Castells, 2009 & 1997; Barnes & Gill, 2000; Bok, 2001; Van de Walle *et al*., 2008; Van de Walle *et al*. (2005); Heintzman & Marson, 2005; Institute for Citizen-centred Service, 2008; National Research Unit, 2009
7. The key antecedents to trusting behaviour are competence, benevolence, integrity, and transparency. Connolly & Bannister, 2007; Bannister, 2007; Mayer, *et al*., 1995; Lee & Turban, 2001
8. An individual's trust in government is related to their own experience of government and public service consumption, personal experiences of family members and friends, and through stories in the media. Institute for Citizen-centred Service, 2008; National Research Unit 2009; Torgler, 2007

9. To public service customers, the impact of a negative experience with a public agency is much more pronounced than the effect of a positive experience.

Kampen, *et al*., 2006

Information Sharing

10. An individual can use a variety of personal 'identifiers' to present herself in a public service relationship.

Lips, *et al*., 2009a; OECD 2009; Camp, 2003; Nissenbaum, 2010; Marx, 2004; Greenwood, 2007; Clarke, 1994; Pfitzmann, 2007; Raab 2005 & 2007

11. What is considered sensitive personal information varies with context and in relationships

Moore, 1984; Nissenbaum, 2010; Schoeman, 1984; Wacks, 1989; 6, *et al*., 1998

12. Individuals' privacy preferences exhibit finely tuned tendencies to disclose, share, and withhold personal information, depending on context, relationship, and type of information.

Olson, Grudin, & Horvitz, 2005: in: Nissenbaum 2010, Halperin & Backhouse, 2008; Lusoli & Miltgen, 2009

Cross-agency information sharing

13. Cross-agency collaboration is not easy, and takes time and additional effort by individuals and agencies involved. The more the clients' needs are interrelated and need to be addressed by multiple agencies, the more government agencies need to collaborate to address their information deficiencies.

Eppel, *et al*., 2008; Lips *et al.,* 2009c; Conklin, 2006; Ritter & Webber, 1973; Bryson, *et al*., 2006; Klijn, 1997; Rommel & Christiaens, 2009; Das & Teng, 2001; Ring & Van der Ven, 1992; Dyer & Chu, 2003; Edelenbos & Klijn, 2007; Muthusamy & White, 2005

14. International research findings demonstrate that there are many cases where a citizen's personal information is still not shared when it should be, or where it is shared when it should not be.

6, *et al*., 2005; Gil-Garcia, *et al*., 2007; Bellamy, *et al.*, 2008; Peckover, *et al.*, 2008; Wetmore, 2007; Bellamy, *et al*., 2007; Taylor, *et al*., 2006;

15. Research shows significant barriers to cross-agency information sharing in organisational, political and legal, and technical domains.

Gil-Garcia *et al., 2007*

16. International research suggests a lack of confidence in corporate governance of organisations responsible for collecting, storing and sharing significant amounts of personal information.

Backhouse and Halperin, 2007

Implications of information sharing

17. Available literature points at two different perspectives on the management of citizen identity information in e-government service environments: a 'Surveillance State' perspective and a 'Service State' perspective (see Figure 4). UK-based research suggests that attributes of both perspectives can be observed in e-government service environments when looking at the actual use of citizen identity information.

Lips *et al*. 2009b

Information privacy

18. Privacy is a multifaceted, ambiguous notion which means many things to many people.

6, 1998; Buchanan, *et al*., 2007; Nissenbaum, 2010; Moore, 1984; Gavison, 1980; Burgoon, *et al*., 1989; DeCew, 1997; Malhotra, *et al*., 2004; Viseu, *et al*., (2004)

19. The meaning of informational privacy is changing under the possibilities opened up by new ICTs.

6, 1998; FIDIS, 2006; Dunleavy, *et al., 2006; Lips, et al*., 2006; 6, *et al*., 2005; Bellamy, *et al*., 2005; Halperin & Backhouse, 2008; Lips, *et al*., 2009b; Taylor, *et al*., 2007; Nissenbaum, 2010; 6, et al., 1998; Birch 2007

20. Concerns expressed about privacy do not necessarily translate to online behaviour.

Nissenbaum 2010; Viseu *et al*. (2004)

21. There is a tension between privacy and the use of personal information to achieve more convenient public services for citizens.

Nissenbaum, 2010;

22. There is a tension between privacy and the use of personal information to support public safety.

Bennett & Raab, 2003; Nissenbaum, 2010; O'Harrow, 2005; Regan, 1995; Roberts, 2004; Zureik, 2008

23. Available literature points at possibilities of 'function creep' or 'mission creep'.

Bennett & Raab, 2003; Koops *et al*. 2007; Clarke 1988; Nissenbaum, 2010; Gellman, 2004

Trust in the e-service environment: information security

24. Robust identity management is identified as an enabler of trust in e-government service environments.

OECD 2009; 6 *et al*. 1998; Lips, *et al*., 2009a & 2009b; Crompton, 2008; Birch 2007

25. Dominant barriers to online public service consumption relate to an individual's perception of risks associated with the online environment.

National Research Unit, 2009; Rotchanakitumnuai, 2008; Kelly & Hopkins-Burns, 2010;

26. Threats to the security of personal information can come from human fallibility, technological fallibility, or from the interaction between human and technological fallibility.

Bennett & Raab, 2003; Lusoli, *et al*., 2009; Schneier, 2004;

Awareness

27. People have little awareness of what personal information is held by public sector agencies.

MORI, 2003; Australisan Communications and Media Authority 2009; Madden, 2010

28. People operating in online environments lack crucial knowledge about privacy practices and available tools.

Viseu, *et al.*, 2004; Buchanan, *et al*., 2007; Madden & Smith, 2010

Experience, skills, ease of use

29. Previous experience, training and skills, and Internet access, support the uptake of e-government services. A barrier to e-government service uptake is familiarity and comfort with existing service channels.

Gil-Garcia *et al*., 2007; Viseu *et al*., 2004; Tsai, Egelman, Cranor, & Acquisti, 2007; in: Nissenbaum 2010

Transparency

30. There is a lack of transparency around ICT-enabled information aggregation and analysis in varying relationships between individuals and organisations.

Camp, 2003; Taylor & Lips, 2008; Koops, *et al.*, 2007; Gandy, 1993; Lyon, 2007; Solove, 2004; Nissenbaum, 2010

31. Transparency enhances the protection and security of citizen identity information by supporting citizens' control over their personal information.

OECD 2008; Thomas & Walport 2008; Lusoli *et al*., 2009

4. Research Findings

In this chapter we provide our analysis of the data. In 4.1 we provide a profile of each of the 10 focus groups. In section 4.2, we present our findings under the analytical themes identified in the literature.

4.1 Group characteristics

There were 63 participants, numbered for convenience 1–63, spread across the ten focus groups. The focus groups were convened in seven locations: six were in major city centres on the North and South islands – Auckland, Wellington and Christchurch. The remaining four were in minor centres, two on each island – Ashburton (population 27,372), Nelson (42,888), Gisborne (44,499), and Stratford (8,889)[1].

The focus group selection criteria aimed to obtain males and females in near equal proportions and a spread of ages and ethnicities.

Each participant was asked how much use they made of the Internet. In keeping with the classifications commonly found in the international literature, these responses have been classified as high for daily use of the Internet, low for approximately weekly use, non-use and ex-use. Each participant was also asked about their use of three different types of e-government services: (1) looking up government information online; (2) interacting with government agencies online, for example through email or participation in online forums; and (3) doing transactions with government agencies online.

The ten focus groups, including the distinctive flavour of the discussion in each group, can be described as follows:

Group 1:

Group 1 consisted of participants 1–6. This Wellington group consisted of three men and three women. There were four pakeha, one Asian and one Pasifika in the group. All were salary/wage earners, in employment, with mid or high income levels. All were high users of the Internet who had accessed some e-government services online. Generally, this group had a good awareness of government agencies and their responsibilities, most of them currently or recently had worked for government agencies. This group distinguished between the action of individuals within organisations, and that of organisations as a whole. They had a largely positive view of government organisations, sometimes in spite of negative experiences.

Group 2:

This group consisted of participants 7–12. They were all salary/wage earners with mid or high income levels in a minor South Island centre. The group consisted of three men and three women, all Pakeha. The group was fairly trusting of government, and would be happy to see a single identifier used for all

[1] All population statistics are from Statistics New Zealand official most recent census figures (2006).

government transactions. They tended to believe that there is more sharing of information between government agencies than there currently is. Also they tended to be more accepting of the use of personal information to monitor for fairness and compliance (e.g. the monitoring of defaulters, fraud/abuse, immigration over-stayers). Internet awareness was low on average, but the convenience factor of 24/7 access was important for people with busy lives. This group had a long list of agencies they are comfortable sharing information with. They were aware of identity theft and wary about what they do over the Internet.

Group 3:

This group consisted of participants 13–17. The three men and two women were all located in a major South Island centre, full time students, under 30 years of age, and with low income levels. There were four high Internet users and one low user. They all had used the Internet for student loan applications. Overall they were a fairly ICT experienced and Internet savvy group. The group had a conversation comparing security face-to-face, over the phone, and over the Internet. Their discussion revealed some subtle, context-specific decision making about channel choice involving factors such as location, time, perceived risk, security and trust.

Group 4:

This group consisted of participants 18–24. There were five men and two women, all Pakeha. They were all middle aged, self-employed business people, with mid and high income levels, located in a major South Island centre. All were high Internet users except one. They were all very familiar with the government agencies that deal with businesses (e.g. IRD, Ministry of Economic Development, Immigration, Customs), and had less awareness of the social agencies (e.g. Housing, WINZ, CYF). They were of the view that government is not working for them and generally its interventions make it more difficult for them. They also believed that the rules should be fair and followed by all. For this group, monitoring ensures fairness and adherence to rules, and a 'fair cop' for those not following rules, avoiding compliance or cheating. They had an awareness of Internet security and identity protection issues. Furthermore, they regarded government as ultimately human and fallible – which made them cautious about trusting government and its agencies.

Group 5:

This group consisted of participants 25–31. The four men and three women were all Pakeha, 65 years or over, receiving national superannuation, and living in a minor centre on the South Island. Income ranged across low mid and high levels. Their Internet use varied: there were high users, low users and non-users, in the group. Across the group they had a positive view of government agencies. Although they are all in receipt of national superannuation payments they had currently relatively sparse, personal experiences of government agencies. They expressed strong views about time use, quality of life and interpersonal relationships: these views explained their preference for face-to-face dealings with government agencies. They valued their privacy and were generally not happy about providing personal information to government agencies.

Group 6:

This group consisted of participants 32–38. This group of four men and three women, all Pakeha, lived in a minor North Island centre and were under 30 years of age. They were all wage and salary earners on a range of incomes from low to high levels. They were mainly low users of the Internet and one was a non-user. They roughly could be divided into two sub groups: females who work in offices and males who work in the field. This appeared to influence issues around channel choice and information sharing: for instance males tended to prefer visiting government agencies and doing their business face-to-face, finding this easier because the people in the agencies knew them and their past histories. The females were more ambivalent. The group tended to trust government organisations because they knew the people they were dealing with. They were also generally happy about information sharing between government agencies.

Group 7:

This group consisted of participants 39–43. These three men and two women, all Pakeha, were all in receipt of some sort of benefit (invalid, sickness or domestic purposes benefit or DPB): they therefore were all on low income levels. They were from a minor centre in the North Island that has higher levels of benefit dependency than average, and also a lower percentage of homes with Internet access than average for New Zealand[2]. The group as a whole had a fair knowledge of the social agencies from their own experience, but less apparent awareness of other agencies of government and what their responsibilities are. There were two extremes in this group – one person with a series of negative experiences and a strong distrust of government and its agencies, and one person with a positive experience of interacting with government agencies. Overall the group tended to view government negatively: as 'out to get them'. This view was also shaped by some experiences of human error and incompetence in dealings with government departments, despite an acknowledgement that 'there have been some nice people'. Overall they tended to favour face-to-face and telephone access to government services.

Group 8:

This group consisted of participants 44–50. This group of three men and four women were all Pasifika (two Tongan, two Samoan, two Cook Is). They were all on low to mid incomes, and based in a major North Island centre. They were mostly high Internet users and one was a low user. Their discussion pointed towards a strong sense of privacy about personal information, particularly financial information. They also indicated a low level of trust in the integrity of individuals in government agencies to treat their information properly. If they had a choice, the Pasifika group would rather that there is no sharing between agencies.

Group 9:

This group consisted of participants (51–56 and 58).This group were all Māori, on low to mid incomes, based in a major North Island centre. This group of two men and five women were all high Internet

[2] Census 2006.

users and had strong concerns about information security. Their discussion indicated mistrust in the integrity of individuals within organisations to deal with their personal information in confidence and according to the law or organisational guidelines. Misunderstanding of Māori pronunciation and Māori place names by officials in government agencies were raised as further examples that undermined this group's trust in government agencies.

Group 10:

This group consisted of participants (57 and 59–63). This group of two men and four women, all Pakeha, were a group of non-users in a major North Island centre. They were all on low incomes. Their discussion revealed some understanding of the Internet. They illustrated this understanding with tales about identity theft and mistaken identity mostly informed by stories they had read or seen in the news media. In their discussion they were questioning about what information is collected and what it is going to be used for. Most preferred a personal approach to doing business. With two exceptions, they did not feel disadvantaged by not being able to work online.

A summary of the group profiles is provided in Table 1.

Table 1: Summary of Group Profiles

Group (participants)	Location	Gender		Age	Ethnicity	Employment	Income Level		ICT Use	e-Government Use		
		Male	Female							1	2	3
1 (1-6)	NI Major	3	3	30-45 yrs	Pakeha 4 Asian 1 Pasifika	Full Time salary and wage earners	H M L	5 1 -	High	6	3	5
2 (7-12)	SI Minor	3	3	30-40 yrs	Pakeha	Full or Part time salary and wage earners	H M L	2 4 -	High 5 Low 1	5	3	3
3 (13-17)	SI Major	3	2	All <30 yrs	Pakeha	Tertiary Students	H M L	- - 5	High 4 Low 1	5	2	3
4 (18-24)	SI Major	5	2	30-65 yrs	Pakeha	Self Employed	H M L	4 3 -	High 6 Low 1	7	3	1
5 (25-31)	SI Minor	4	3	+65 yrs	Pakeha	Superannuitants	H M L	2 2 3	High 4 Low1 Non-User 2	2	1	-
6 (32-38)	NI Minor	4	3	20-25 yrs	Pakeha	Full time salary and wage earners	H M L	2 4 1	Low 6 Non-User 1	5	-	3
7 (39-43)	NI Minor	3	2	40-50 yrs	Pakeha	Beneficiary	H M L	- - 5	High 1 Low 1 Non-User 3	2	1	1
8 (44-50)	NI Major	3	4	20-55 yrs	Pasifika	Full or Part time salary and wage earners	H M L	- 4 3	High 6 Low 1	5	2	2
9 (51-58)	NI Major	3	4	30-65 yrs	Maori	Full or Part time salary and wage earners	H M L	- 4 3	High 7	5	2	3
10 (57-63)	NI Major	2	4	45-65yrs	Pakeha	Part time salary and wage earners - 3 Beneficiary - 1 Superannuitant - 2	H M L	- - 6	Low 1 Non-User 4 Lapsed 1	-	-	-

4.2 Thematic analysis

In this section, the responses of participants in the focus groups are described and analysed under the themes identified in the literature review:

- Individual's acceptance and use of the Internet
  - Age
  - Ethnicity
  - Geographic location/community
  - Level of Income

    - Employment
    - Education
    - User acceptance of e-government service provision
- Channel choice
- Trust in government and/or the public service providing organisation
- Information sharing including
    - Information relationship between the individual and the public sector
    - Cross-government information sharing
    - Implications of information sharing
- Information privacy
- Trust in the e-service environment: information security
- Awareness
- Experience, skills, ease of use
- Transparency/openness

4.2.1 Individual's acceptance and use of the Internet

In the international literature, a distinction is made between high and low Internet users, non-users and ex-users. Therefore our research participants were asked about their current use of the Internet. Of the 63 participants, 39 people identified themselves as high users, accessing the Internet more or less daily; 13 people were low users, using the technology approximately weekly, and 11 people were non-users. One of the participants had formerly been a user but was now happy to have others (e.g. mother) access information from the Internet and do e-transactions for her. In this section we examine Internet use and e-government use against the participant characteristics of age, culture or ethnicity, geographic location of the community where the participant lives, level of income, and education. This is followed by a more general analysis of the data for individual's acceptance and use of the Internet.

4.2.1.1 Age

Age of the participants was considered in three bands: Under 30 years of age; 30 –64, and 65 years and over. These age bands were used to look at variations in Internet use and e-government use between age groups.

High, low and non-users of the Internet were found in all age groups as shown in Table 2.

There were 14 participants under 30 years of age. They were mostly in two discrete focus groups: the student group in a major South Island centre; and a young wage and salary earners group in a smaller North Island centre. Two participants from other groups who were 30 or younger, have also been included for the analysis that follows.

Table 2: Internet usage by age groups

Internet Use	Age	
High (approximately daily)	<30 yr	5
	30-64 yr	29
	+65 yr	5
Low (approximately weekly)	<30 yr	8
	30-64 yr	4
	+65 yr	1
Non-User	<30 yr	1
	30-64 yr	6
	+65 yr	3
Ex-User (Lapsed)	30-64 yr	1
Total		63

These younger participants included six high Internet users, seven low Internet users and one non-user. Even the one participant who identified himself as a non-user had looked up government information online and done transactions with government agencies online.

There were nine participants 65 years of age or over. Four of these people were low or non-users of the Internet and the remainder were high users. Three had low incomes and the remainder were on medium or high incomes. Computer and Internet use appeared to be more of a life choice than income related. Participants spoke about not wanting to spend time on the Internet, even though they could afford to financially, and would be capable of doing so [30].

Participants were also asked whether they have ever made use of the following three types of e-government services: (1) looked up government information online; (2) interacted with government agencies online through email or online forums and the like; or (3) done a transaction online with a government agency (e.g. registering a car, applying for a student loan, enrolling in Kiwisaver). More than two thirds of the participants had used at least one of these services and eleven participants had used all three. The reported use of e-government services in all age groups is shown in Table 3.

Table 3: Use of e-Government services by age group

e-Government use - Age

E-Govt Use	Age	
Looks up Public Sector information online	<30 yr	12
	30-64 yr	27
	+65 yr	3
Interacts with Government agencies online	<30 yr	3
	30-64 yr	13
	+65 yr	1
Does transactions with Government agencies online	<30 yr	8
	30-64 yr	13
	+65 yr	0

4.2.1.2 Ethnicity and culture

One focus group consisted entirely of Māori participants (Group 8) and another entirely of Pasifika peoples (Group 9). There were also one or two people in other groups who were Māori or Pasifika. The eight Māori participants were all high users of the Internet. The eight Pasifika participants consisted of seven high users and one low user of the Internet. There was one Asian participant, a high user of the Internet. The remainder of the participants were 46 Pakeha, consisting of 23 high Internet users, 12 low users, 10 non-users and one ex-user as shown in Table 4.

Table 4: Internet use by Ethnicity

Internet Use	Ethnicity	
High (approximately daily)	Pakeha	23
	Maori	8
	Pasifika	7
	Asian	1
Low (approximately weekly)	Pakeha	12
	Maori	0
	Pasifika	1
Non-User	Pakeha	10
	Maori	-
	Pasifika	-
Ex-User (Lapsed)	Pakeha	1
Total		63

The use of e-government services by different ethnic groups is shown in Table 5. Two thirds of participants had looked up public sector information online, 29 Pakeha, seven Māori, six Pasifika, and one Asian. Less than a third of participants had interacted with government agencies online, 12 Pakeha, two Māori, and three Pasifika. A third of participants had done transactions online with government agencies, 14 Pakeha, four Māori, and three Pasifika.

Table 5: E-Government Services Use by Ethnicity

E-Govt Use	Ethnicity	
Looks up Public Sector information online	Pakeha	29
	Maori	7
	Pasifika	6
	Asian	1
Interacts with Government agencies online	Pakeha	12
	Maori	2
	Pasifika	3
Does transactions with Government agencies online	Pakeha	14
	Maori	4
	Pasifika	3

4.2.1.3 Geographic location/community

The data were examined for similarities and differences in Internet use and e-government service use of participants from the three major city centres (N=37), and the more minor population centres (N=25). High Internet users were found in all communities. Low and non-users are more common in the North Island groups. This is probably mainly a result of the location of particular focus groups, such as the non-user Group 10 in Auckland. Also Stratford, one of the North Island minor centres, is a much smaller centre than the other minor centres and all the participants in that group were low users or non-users of the Internet.

Among the non-users, time required to access computers and find relevant information online, customised to an individual's particular circumstances, was often mentioned as a reason for non use.

Table 6: Internet use by geographic location

Internet Use	Location	
High (approximately daily)	NI Major	19
	NI Minor	1
	SI Major	10
	SI Minor	9
Low (approximately weekly)	NI Major	2
	NI Minor	7
	SI Major	2
	SI Minor	2
Non-User	NI Major	4
	NI Minor	4
	SI Major	-
	SI Minor	2
Ex-User (Lapsed)	NI Major	1
Total		63

4.2.1.4 Level of Income

Participant personal income was collected in bands of low (under $35,000 p.a.), two middle bands ($35–$45,000 and $45–$55,000) and high (greater than $55,000).

Twenty six participants were in the low income band and some were found in all groups except three: Group 1 (NI major, employed); Group 2 (SI minor, employed); and Group 4 (SI major, self-employed). Fourteen participants were in the high income band and these were more tightly clustered in five groups: Group 1 – 5; Group 2 – 2; Group 4 – 3; Group 5 – 2; and Group 6 – 2. Income was not closely matched to age (Table 7), although all the beneficiaries and students, as might be expected, had low incomes.

Neither was high Internet use closely associated with income level (Table 8). There were both high and low personal incomes among the high and low Internet users. Cost of using the Internet was not mentioned by any recipients although most of the non-users were in the lowest income band.

Table 7: Income level by age bands

Age - Income

Age	Income	
<30 yr	<35K	8
	35-55K	4
	Over 55K	2
30-64 yr	<35K	14
	35-55K	16
	Over 55K	10
+65 yr	<35K	4
	35-55K	3
	Over 55K	2
Total		63

Table 8: Internet use by income bands

Internet Use	Income	
High (approximately daily)	<35K	11
	35-55K	18
	Over 55K	10
Low (approximately weekly)	<35K	6
	35-55K	4
	Over 55K	3
Non-User	<35K	8
	35-55K	1
	Over 55K	1
Ex-User (Lapsed)	<35K	1
Total		63

4.2.1.5 Education

The majority of the participants were formally educated to the end of high school, with only a small number having post-school diplomas, certificates and degrees (Table 9). There appears to be no relationship between education level and Internet use. Neither was there any discernable relationship between attitudes to privacy and information sharing and education level.

Table 9: Internet Use and Education

Internet Use	Education	
High (approximately daily)	High School	23
	Diploma	5
	Trade	5
	Graduate	3
	Post Graduate	3
Low (approximately weekly)	High School	6
	Diploma	3
	Trade	3
	Graduate	1
Non-User	High School	10
Ex-User (Lapsed)	High School	1
Total		63

4.2.1.6 Internet awareness

Participants had a broad awareness of the Internet and the services they could access through it. Most Internet-using participants used the Internet to find information, mentioning Facebook and Bebo as examples.

> We just grew up in a generation where it's kind of normal and everyone puts your woes and stuff on Facebook and everyone knows about it. [14]

Many users mentioned the availability of Internet banking and doing online banking transactions.

The older, super-annuitant participants also revealed some awareness of these services but their personal use of them appeared more limited. The older group explained that they made deliberate choices about the time required to obtain information and work online, preferring to use their time in different ways (gardening, sports, family, face-to-face interaction). Some mentioned using the Internet to keep in touch with family but this did not transfer to use of the Internet for accessing government services. Non-users tended to have a generalised awareness of risks associated with Internet use, mostly drawing on anecdotes from the media or other people, and this reinforced their disinclination to become users.

> We don't always trust the way the Internet works. We don't always trust how some people are using it. It's been proven to be flawed. [28]

> It's not for us. [25]

4.2.1.7 User acceptance of e-government service provision

All the groups discussed their experiences of accessing government services over the Internet. Acceptance and use of e-government services provision is shown in table 10. It was highest among the

high users of the Internet but low and non-users had some experience. In some cases participants had asked others (e.g. mother, husband) to access the service for them.

Several users mentioned finding information about government services available to them through the Internet and downloading forms to enable them to see what information they would need to provide. These same people would not necessarily follow through by doing a particular business transaction with the government agency online. They described how they would use the information they gathered to make sure that they had the relevant and qualifying information they needed to provide to the agency, and then they would do the transaction face-to-face by visiting the government agency or doing the transaction over the telephone. Reasons cited for this choice were that people found it easier, over the phone or face-to-face, to obtain information specific to an individual's case, ask questions, or seek confirmation.

Table 10: Internet use and use of e-government services

Internet Use	E-Government	
High (approximately daily)	1	32
	2	14
	3	17
	NA	6
Low (approximately weekly)	1	9
	2	3
	3	3
	NA	4
Non-User	1	1
	2	
	3	1
	NA	9
Ex-User (Lapsed)	NA	1

1 = Looks up Public Sector information online
2 = Interacts with Government Agencies online,
3 = Does transactions with Government Agencies online

Among the 17 participants who had communicated with government agencies through email or participated in online feedback or discussion sessions, a number referred to the time delays involved in conducting business this way. They said weeks could elapse between questions asked, answers, points of clarification and final resolution. As a result some had concluded that it was easier to use the phone or face-to-face channels for all but the most straightforward cases.

There also appeared to be a virtuous cycle in which non-users become users and low users become higher users through positive experiences. Knowledge of a particular e-service led to first use. For a number of users this had been Facebook, Internet banking, or a Student Loan application. Positive first use experience led to trust and further use. For example, one participant who was benefit-dependent had been assisted to access a student loan through Studylink. Her positive experience with Studylink had led to her exploring further services online.

Knowledge of and acceptance of the Internet has links to channel choice, trust in the e-environment and trust in e-service transactions discussed in sections 4.2.2 and 4.2.6. For example, the younger student group tended to have a higher knowledge of the technology, a high trust in the e-environment and e-transactions. They gave examples of happily transferring their trust from one use to another.

4.2.2 Channel choice

Interactions with government agencies include obtaining information to inform availability of services and criteria for access to those services, and transactions to commence service delivery. The available channels for interacting with government agencies include the traditional channels such as visiting of an office and dealing face-to-face with an agency employee; using the telephone to contact a specific person, office, or a call centre; and newer communication channels such as obtaining information about services and eligibility criteria from a website; downloading application forms and information from a website and then submitting application through post or face-to-face; and applications for services made wholly online.

The focus groups talked about all of these channels and discussed what they saw as the benefits and drawbacks, and also when and why they might choose a particular channel.

Channel choices can be different according to circumstances and what is required appears to be influenced by a web of interacting factors. Personal preference for how individuals like certain sorts of business to be done was a factor.

Many participants [e.g. 25, 28, 29, 40, 41, 49] talked about wanting to see the person they were dealing with.

> I feel more comfortable talking to a person individually than talking over the phone or over the computer. I think it's the personality – you can judge the other person that's judging you. [40]

Convenience played a part in influencing users towards online channels.

> Online … It's quick, it's easy, I don't have to leave home. [18]

> If you get half way through and realise you don't have a piece of information you can get up and grab it, whereas it's not always as easy on the phone. [3]

Channel choice is dependent of the services the individual needs and how well they know what they need.

> Depends what you want. If you want information – if you can sieve through it – generally you are probably quicker to find it yourself on the government website. But they can be a bit of a minefield if you don't know exactly what it is you want. [18]

For experienced users of the Internet for access to government services, it was clear that they appreciate the control this gives them, and the anytime anywhere factor.

> I prefer to do it online. [I control] when, how long, and the information I provide … I work nights so you know it's much easier for me to fill on a form in the middle of the night than it is for me to wait until the next morning to ring someone and answer by phone. At least online it's written as well and [online] has the facts, it should be if they got it right. The amount of times you ring up different people and they give you different answers. [3]

> 24/7 being able to go late at night, fill in the form, or register online for something or other. As long as there is like extra comments or a note area, to make it a little bit more personal what you are actually asking. Otherwise, sometimes the form that you are filling out online is just a general sort of thing. [6]

It was clear that human interaction with government agencies has features that people, across age groups, want and value. For most super-annuitants and beneficiaries, non-users, and some others, this is their channel of choice.

> So for me, most of the time, I prefer to speak to someone. [21]

> Push comes to shove, I want to talk to somebody…. I wanted to know that that person has the authority to make the decision on whatever I'm asking [18]

For others, face-to-face is the last resort. It is used only when the individual cannot get a satisfactory response online. This can be because in the individual's view, their circumstances do not 'fit' the form, or online boxes, and warrant a conversation with someone. Several people commented that online forms do not provide the opportunity for individuals to provide information they think might be important. They can only provide what the form allows, hence the resort to face-to-face communication. This lack of customisation was commonly mentioned by high users.

> When something goes wrong for me, on my side, I'd rather go inside and face them to face. [49]

> It's faster to talk to somebody on the phone and get 7 answers than have a string of emails that take ages to come through [17].

Channel choice was affected by the need to ask questions and get feedback and reassurance during the transaction.

> I feel then I've got the other person at the other…. at the other side of the desk for me and we just do it. [62]

> I'll just get on my laptop and it's just way easier. It's just right there for you! You kind of know that if you go in it's going to be done quicker and you can ask any questions but I guess it's a lot easier to use [14].

Asked if the online, face-to-face or phone channel made a difference to what information people were happy to provide, participant's had reasons they would choose all of the channels, for different purposes, at different times. For some sensitive information, face-to-face is seen as safer.

> It feels a bit safer though, doing it in person, over the phone rather than on the Internet, like putting in your credit card number and stuff like that. Swipe your card in front of me … feels safer than putting it on the Internet. [34, 38].

> Sometimes even people who have done transactions online prefer to go into the office [32, 35].

> It's far faster [32]

> It's all the login [that slows online down]. [35] Having to do the security checks over the phone to set up your login.[32] It's just because everything's a different site. So, you've got to log into that site to do that thing and then you've got to log in to [another site]. [34] … then you go back and you don't know what that password was. May as well make a new one. Another phone call for a security check. If it was [only] as easily as click. [32]

Talking to a human rather than a machine on the phone is considered a good second best.

> You can't see them, and you're still talking to the person. You're still talking to a staff member. I think that's what makes it the same [32].

Many thought, on balance, the Internet was preferable to the 'automated thingy' which was seen as 'frustrating' [36], 'slow' [34], and 'not like talking to a person' [32].

These same people, asked what would make them choose online for their first preference, replied:

> If it was quick and fast … I'd definitely go online. [34] If it was easy. [32]

Asked how they would like it if there was one website for all the government they said:

> 'that would make life a lot easier' [32,38,35], 'you could probably use it more, so you wouldn't have the complications '[32]. Others thought that would still be too much hassle and they would still prefer to 'go to town and get it done'. [36].

People made comparisons between the channels based on their experiences. For instance, the phone channel has its pluses:

> They know what they're doing [36].

And minuses:

> The waiting. You get put on hold [34]. Sometimes you get three or four songs [hold music] [35]

Several people wanted a record of their transactions and they thought this was less available when transactions were conducted over the Internet [54].

> I wouldn't mind giving it by email – wouldn't mind sending it in by email, but don't know about the [Internet] … [On email] you're writing it down. You know what you've got written and you've got recourse to do it again if you want to. If they come up and say you said so-n-so, you say hang on, I've got it all written down here what I said to you…. It's the same with a lot of stuff when you write a letter to someone. Take your own copy, if you're after something. If people come back and say you said so-n-so, you say no I didn't – here's the letter. [25]

People unable to access the Internet were asked if they felt disadvantaged by not having that channel open to them.

> Yes [59]. No, I don't. [57, 63] It doesn't bother me [62, 63]. If I want anything online, I can just get my mother to do it [61].

For a few non-user participants, their non use was a more deliberate choice.

> I've got an up to date computer and my boy uses it and I know how to use it but I don't go near it.... I wouldn't stick any of my banking details … on the computer about myself. [39]

Many participants described their preferences for a multi-channel approach, depending on the complexity of their personal circumstances, their knowledge of the services available to them, and the services they need.

> I would call them first, and probably go in, and probably use the Internet last. I just like calling because it's faster and I wouldn't have to go into town to do that but I prefer just talking to them

> face-to-face so that you know things get done quicker, if you ask questions on the Internet it might take longer to reply [16].

> I'd like to access information and get my forms online. But I want to be able … if I fill out with my writing, I want to keep a copy of what I've given. I've only done a couple of transactions online – a lot of them I wouldn't do online. [54]

> Some of their online services can be a bit … I like to ring them…. Ring them, you can ask what forms you actually need to download. They'll tell you the numbers and you can just do it, fill them in and it's done. [8]

Some participants particularly valued the face-to-face experience as 'more personal', leading to a quicker and more satisfactory outcome even when they had access to the Internet and were identified as high users. The reasons given for this were a complex interaction of factors. For example, one group of younger participants (under 30) located in a minor North Island centre told us that they preferred face-to-face contact because it was more personal, easier to get the services they required because they were 'known'.

> It depends on context, because if you go into an office or whatever and it's someone that you know then you're going to trust that person. If you go online, and it's all set up and easy, then online is going to be better. Just like if you have to talk to someone in the city you've never seen before, you're not going to trust that person, and if there's a really cruddy Internet thing that seems dodgy then – so, it just all depends on how it's done, I reckon – what the context is. [32]

Pasifika participants generally had a preference for face-to-face interaction with government agencies.

> I'd rather be speaking to someone face-to-face and giving them all this information and all that, rather than phone or online and all that. [50]

Some participants found a form of anonymity in using the Internet [15, 43] which made it easier to share personal information.

> Computers … give me a sort of feel like there is no human going to be really involved. It gives you kind of this lifeless feel, so you feel like if it's asking you just some random question about your ex-wife and what's her name. You think – 'alright lifeless entity, you can have this information. What are you going to do with it you are not even real!' – That's how I kind of feel [15].

This anonymity is welcomed by some who are required to disclose distressingly personal information which they are too embarrassed or shy to tell face-to-face.

> It's impersonalised. That's why I like the computer. I filled out all my DPB and all the pre-interview on the computer because I couldn't face going in, I was so distraught at the time. It was a lot easier to have a lot of information already there. [43]

Channel choice was affected by people's skills and knowledge.

> Elderly chap at work had no idea how to use a computer. [For him] to download a form is the scariest thing out. [8]

> Don't ask my wife she has trouble, she wouldn't know how to click on the address on the emails [12]

> I don't do computers so anything to do with computers... forget it. [42]

Peoples' options for channel choice can be limited by their access to a computer and the Internet:

> But not everybody has a computer… not everybody can access… you know… you're still going to be stuck with that. [46]

> You know – someone that doesn't use the Internet day in and day out – they're not just going to go on there to do something they needed [34].

> [My husband] does everything like that for me. I would be capable of that, but he just does it – and because we are the last people to get the latest in gadgets, machinery and technology – we have a very old fashioned streak in us, partly because we don't want to spend time on those sorts of things, but because of that we don't have the Internet, and sometimes we feel a little bit out of it. [30]

People working and living in some of the minor centres saw their channel choice as part of their social networks, and therefore favoured face-to-face [32, 36, 39].

> It depends on what you query as well. Like, if you've got a difficult question and you go on the Internet and it will take ages to find the answer sort of thing. Whereas, if you go to a person, they're going to know straight away [34].

> I would use the Internet to look at the forms, get instructions, things like that, and end up writing it out and then filling it out and sending it back. It also gives me time to think about what I've already done, double check it [24]

People in smaller centres noted the advantages of 'being known' which can tip their choice towards face-to-face and phone contact.

> It depends on what you're used to. You know, if you're used to going and seeing somebody all the time and it works well, why are you going to change to the Internet? You'll have to build that trust up. [37].

> It would be different in small towns because of their size. If you're in a city, well you're not going to know from one shop to the next people – where here, we know everyone. So, for us it's probably faster, where for a city person it's all going to be as fast as each other [32].

> I think it's easier to go into a shop than to have to go onto the Internet and find what you're looking for…. You can see the basic stuff on there, but they never are. They're filled with all sorts of crap around it. If it was just a basic thing about [what you are wanting to do] [34]

Age did not appear to be a major factor in channel choice. There were low users of the Internet among the younger group and some of them preferred face-to-face contact even though they were high Internet users. There were also high users of the Internet among the older participants although this did not necessarily determine their channel choice.

> Older participants generally preferred face-to-face interactions with government agencies because they valued to opportunity to see the person they were dealing with.

> It's a personal touch – you can trust people. We don't always trust the Government. [29]

Some high Internet users among the older participants were open to using the online channel for e-government transactions, and had previously done so.

> I wouldn't mind giving it by email – wouldn't mind sending it in by email, but don't know about the other. [25]

Younger people were quite diverse in their preferences for channel choice and their reasons had to do with convenience, what they were used to and the maintenance of established patterns and relationships.

> It depends on what you're used to. If you're used to going and seeing somebody all the time and it works well, why are you going to change to the Internet? You'll have to build that trust up. [37]

4.2.3 Trust in government and/or the service providing organisation

Participants varied in the extent to which they trust government and the reasons they provide for their trust or distrust. A number of participants, particularly among the younger ones did not make much distinction between agencies of government and government as a whole.

It appeared that the younger participants (under 30 years) had experienced only a small number of government agencies and services for themselves. Older participants (65 years and over) interacted with only a limited number of government agencies. Both groups were more likely to think of government as a holistic entity and make little distinction between the roles and actions of its various entities. On the other hand people whole interacted with a wider range of agencies experienced first hand the operational separateness of the various organisational arms of government.

> I think we'd like to think (of government) as one organisation, but when you deal with them you deal with so many different facets suddenly doesn't feel like it a cohesive entity, like a whole bunch of entities playing in their own little paddock depending what department they are in. [18]

Participants generally had a view of the New Zealand government and its agencies as benign and working in their interests.

> New Zealand has a relatively nice government … if I lived elsewhere I'd be a little more concerned…. I assume government is not going to use my information to harm me in any way, unless I have broken the law or something like that … you don't really have to worry unless you have something to worry about. [13]

For some participants, the government agency brand alone can be enough to generate trust.

> Just the fact that they are government services – you think 'well these are trusted". If it was some sort of dodgy insurance company, I might have a second thought … but you instantly compare the government as being relatively controlled and safe – in New Zealand at least. [14]

Younger participants tended to trust government agencies and the government brands.

> If we can't trust them, who can we trust? We should be able to trust what they do. [37]

Some participants made it clear that trust in the service providing organisation and performance go hand in hand.

> If you are dealing with the online and the website constantly crashes, or ring up (for something) and it hasn't arrived, you'd be less likely to trust them. But if their online processes work efficiently, then again you have less reason to distrust. [5]

Older participants made a distinction between government departments which can be trusted and those not to be trusted. Its various roles might also affect people's attitudes positively or negatively according to circumstances.

> Some Government Departments are there especially to protect the public and individuals. Others are there to – and they will all say that they are – protecting and serving the country and individuals. But some are seen to be doing that more than others. Some are seen to be making your life difficult, and therefore you're not going to feel so warm towards them. [28]

Major centre participants on both the North and South Islands had concerns about the competence of individuals within some government agencies. They perceived a lack of accountability for the actions (or inactions) of individuals and the organisation.

> We want to trust their system. We want to trust and we expect that if someone works for the government they are trustworthy, but ultimately, at the end of the day they are still human. There's both the incompetent and the untrustworthy. [18]

> All these departments depend on the personnel that are running it and the common sense that these people have got – unless they have good people you may as well not go – you are wasting your time (dealing with them). [25]

While acknowledging that there are good people in government agencies who go out of their way to be helpful, there were many comments about the use of the power of position which left participants feeling very negative about government agencies.

> Some people go right out of their way to help you and some of the people go right out the way to make sure (they don't help you). It's almost like they've got no life of their own so here's their one moment to go bam, got ya! … They never tell you the full story about something – is that because they are concerned about their job, or is that because they are concerned about statistics. [18]

Older participants perceived the need for front-line staff to have discretion to listen to and take account of the particulars of the case in front of them. To them this goes hand-in-hand with trust.

> All these departments depend on the personnel that are running it and the common sense these people have got – because a lot of them haven't. You go to get something done in one of these departments and somebody puts everything in your way that's got nothing to do with the issue, instead of coming out and saying – 'yes this is an unusual case' – use a bit of common sense and let it go through, but they don't. – none whatsoever. So to me, unless you've got good personnel in a lot of these places, you might as well not go. You're wasting your time. [25]

The South Island based self-employed participants (Group 4) and the wage and salary earning participants also based on the South Island (Group 2) tended to the view that government's interventions were generally not helpful and in their interests. On the contrary, they thought government generally makes life harder for individuals and they were therefore less inclined to trust that the actions of government agencies are in their interests.

The participants who expressed distrust in government agencies were extremely strong in their feelings. For instance, one benefit-dependent participant introduced himself with the statement 'I don't like government'. Participants who distrusted government agencies were most common among the benefit-dependent, Māori, and Pasifika participants. Their distrust was often illustrated by negative service experiences.

> They tried to put it across me that they never received my track pack (traceable mail) and it took me 10 days to force them to admit that they'd received it. [39]

Distrust of government agencies was particularly marked in participants who had a continuing service dependency on government agencies such as beneficiaries and Working for Families Tax Credit clients. Most of the individuals in these groups who expressed their distrust in government agencies linked their distrust to the actions of individuals, but their distrust of individuals was generalised to the organisation.

Among Māori, Pasifika and beneficiary groups generally, there was a feeling of powerlessness in dealings with government agencies.

> It doesn't matter whether you like it or not. In order to get what you want, you've got to give them … all the information….and sometimes you feel like you don't have those rights into your personal rights… but, you won't get what you want if you keep holding back. [44]

Māori participant's trust in government agencies was affected by the service experience they or close members of their family had received.

> That's happening to my brother – he's a sickness beneficiary. Every time – he goes to the doctor, gets assessed – he gets three months – but there's one particular woman in there who's badgering him and saying there's nothing wrong with you – get out and get a job- keeps misplacing his calls. This is WINZ. Every three months when he goes in, there's always an extra two or three weeks he has to wait to get paid, and it pisses him off and he gets upset, and you know, I don't believe that particular woman – she should be sacked. She shouldn't be questioning the patients, you know. She's there to do process. You know what I mean? The doctor does his job. You know what I mean? So, those people have got too much to say. [55]

As a group, Māori particularly had doubts about whether the processes operated by organisations to protect privacy of information are sufficient for them to trust the organisation. They had a low level of trust in the integrity of individuals within government agencies and this distrust, for them, was extended to the organisation. Exceptions to this generality were found in individuals who work or have worked for government agencies and consequently have a higher level of administrative and service awareness [52].

Māori participants saw understanding of New Zealand English and particularly Māori place names as an important competency for all the people they have to deal with in government agencies.

> What I do have a problem with– is either on the phone, or dealing with somebody directly – is dealing with someone who can't really cope with the language. (Group agreed in unison) – How do you spell your street? How do you spell your name? [58]

Some participants, particularly those in Group 1, despite some negative experiences, separated the service failures of individual staff from the organisation as a whole, and were inclined to trust the agency, even if some individuals sometimes did not follow procedures or misused private information.

> I guess we trust the agency more than the person. It seems to be more often that the person gets the information wrong rather than the system. [5]

The positive experiences of clients with some services, for example Studylink, seem to have built trust and confidence. The Studylink example illustrated a case where an organisation had taken the step of communicating their approach to security to their clients and upgrading their security and explaining why, had a positive effect on client trust in the organisation and the channel.

> I would go with the online one – especially Studylink because they have upgraded their security so much in the last year. You have to have your number, your password and then you have to have a special … pass code. [17]

4.2.4 Information sharing

Participants gave many examples of the kinds of information they are asked to share with government agencies. This ranged from the core information of name, address, date of birth, telephone numbers which are required by nearly all the organisations participants experienced, to information of a more specific nature, such as IRD number, employment status, income, health problems, details about family size, household composition and other specific personal and family details according to the services being sought. We have organised the research findings under three different areas of the discussion: 1) the information relationship between the individual and the public sector; 2) cross-government information sharing; and 3) Implications of information sharing.

Information relationship between the individual and the public sector

Participants were aware of the way agencies use specific information to identify them as individuals and see benefits to them personally in this.

> That's how they confirm the identity for a start. [10]

For example, when ringing IRD, customers are asked to key in their IRD number. However, participant's perceptions were that this information is not remembered by the system and some asked 'why bother?' if they are going to be asked for the same information again later during the transaction with individual officers [10, 12].

In the view of many participants, the information they provide government agencies does not appear to be used in a way that acknowledges previous exchanges, even by the agency they gave it to, leading to much duplication of information provision.

> You can spend two days on the phone and the first person you tell them the whole situation, and then it's over and over…. so you're repeating.[60]

Participants sometimes understood the need for this information to establish identity and service eligibility, and the conditions under which such information is provided.

> They are only supposed to use it for the purpose that you give it to them for. They are not supposed to share it or keep it and use it for other purposes, so they should just use it once, and I think it's probably why you have to keep giving the same information again and again because they are not allowed to just share it with their colleagues [6]

Many high users of government services (students, beneficiaries, Kiwisaver, Working for Families Tax Credits) mentioned that they found this process 'pretty repetitive' and 'frustrating' and expressed a wish that agencies were better at recognising and 'remembering' or 'recalling' previous interchanges.

> One of the most frustrating things that I found over years of dealing with government departments … is every time you go into one, the first thing they do is they give you a form and you've got give your name, your address, your birthday, your phone number, every single time…. You shouldn't have to do that – not with the technology that's around these days. [20]

Many also noted the duplication of provision of information provided to government agencies e.g. ACC, WINZ and IRD.

> Pretty much every form that you fill out – it's the same sort of format. Doesn't matter what sort of accounts or departments you go for. [10

It is not accepted that the use of client numbers delivers anonymity all the time.

> You usually get a number, but then that number can still get traced back to your name. [17]

People in receipt of certain services were aware that information they might consider private, such as income, is required by several agencies. One [8] gave the example of AAC, WINZ and IRD all having income information for anyone in receipt of ACC. Their comment was since they all have it anyway, why can't they share it.

Some thought IRD number already had some of the characteristics of a client number that operates across several agencies.

> You can't get WFFTC without your kids having an IRD number. To get a bank account you need an IRD number. I just opened a bank account for my 1-year old – we had to get him an IRD number … so already IRD number is like a social security number [8]

Some, particularly among the younger participants, expressed a wish for a single process for managing their identity when dealing with government agencies.

> I'd love to be able to just give a number and never have to repeat it. [9, 8]
>
> With the technology these days it should be possible to do. [7, 10]
>
> How many numbers do you need – ACC, WINZ, IRD, health, drivers licence, passport. [7,8]

In a group exercise during the focus groups, the participants were shown a list of government agencies and asked to sort them into agencies they would be comfortable sharing information with and those they would be not comfortable sharing information with. The results of this discussion are summarised in Table 11.

Table 11: Comfort/discomfort with information sharing by government agencies

Group	Comfortable		Uncomfortable	Don't Know
1	LTSA, Police, DHB, MoE, DIA, Justice, Immigration	ACC, IRD, WINZ, Companies Office	CYF, MfE, Housing	Customs, Law Commission
2	CYF, WINZ, Housing, IRD, ACC, Customs, MoH, Office of the Ombudsman, Immigration, Police,	Dept of Courts, SFO, DoL, DIA, MoJ, MED, Crown Law Office, Archives, Government Superannuation Fund Authority	Immigration, Lotteries Commission, NZTE, Crown Law Office, Charities Commission, Accounting Standards Review Board, MoT, MoJ, MFAT, Mfish, MfE, MoE	
3	**Know what they do** Statistics, Police, MoE, ACC, Mfish, Housing, SFO,, CYF, WINZ, MoT, IRD, MoJ, MAF,	Charities Commission, Treasury, Immigration, Government Superannuation Fund		**Don't know** Securities Commission, Office of the Ombudsman, OPC, Customs, NZTE, Archives, Crown Law Office, MED, Electoral Commission, Accounting Standards Review Board, TEC, Dept of Courts, MfE, MSD, Takeovers Panel, Law Commission, Commerce Commission, Retirement Commission, MFAT, DoL
4	Crown Law Office, Police, SFO, ACC, MFish, Housing, CYF, WINZ, MoT, IRD, MoJ, MFAT, DIA, MoH, Office of the Ombudsman	Customs, Archives, Law Commission, Immigration, Commerce Commission, Electoral Commission, Securities Commission, Retirement Commission	Statistics, MoE, Charities, MAF, Treasury, MED, NZ Lotteries, OPC, NZTE, TEC, MfE, DoL, MSD, TEC, MfE, Government Superannuation Fund Authority, Accounting Standards Review Board, Takeovers Panel	
5	NZ Police, MoT, Customs, ACC, Lotteries , Securities Commission , Charities Commission,	Retirement Commission, Archives, MFAT, TEC , Law Commission MoH , WINZ	NZ Police, OPC, MoJ, Dept of Courts, Immigration	The group didn't reach a view about MSD (WINZ, CYF)
6	IRD, ACC MoT, Police	Immigration, WINZ DIA, MoJ	Courts, StudyLink, CYF, Mfish, MSD, Housing, MAF, MoE, DoL, SSC, MfE	
7	Statistics, DoL, MoE	StudyLink, MFish	MoJ, DIA, WINZ, Housing, Courts, MoT, ACC, IRD, MSD, CYF, Police	Immigration MfE, MAF
8	StudyLink (100%) ACC (100%)	Housing (100%) MoH (75%)	IRD (0% comfortable)	Police (50-50%) MoJ (50-50%) Immigration (50-50%) Mfish (50-50%), MoE (50-50%),
9	MAF, MoT, Statistics, Mfish, MoH, MfE, MoE OK – but only basic info: name, address, phone number, DoB		ACC + DoL + IRD: May not be able to qualify for any ACC payment because of any payment made from DoL or IRD Courts + WINZ: I have no say over how much comes out of my benefit to pay fines	
10	Courts, CYF MoJ+Police WINZ+Housing	MoH+ACC Immigration IRD	Police, CYF, WINZ	

There was generally a lack of awareness about government agencies and their roles except where individuals have experience of them directly, or through close friends and family. The beneficiary participants tended to know about WINZ, ACC, Housing and IRD. The self-employed group had encountered Customs, Agriculture and Fisheries, Companies office in Economic Development. The student participants knew Studylink and visible agencies like Police but few others. The general conclusion across all the groups is that participants are uncomfortable about sharing personal information with government agencies they did not know and understand what they do.

Because of their low level of knowledge of the agencies the students discussed information sharing on the basis of their knowledge of the agencies. If they knew what they did then they were generally comfortable with them sharing information.

The remaining groups used various strategies during their discussion to make a decision. Some groups (2, 4, 5, 10) clustered the agencies because they thought they 'go together' because of the type of business they did and sharing information would be good because it would make the agencies more effective and efficient. This was sometimes based on participant's experience that some agencies already share information (such as ACC – WINZ – IRD) or because people thought that they would have a better experience as service clients if they did. A common cluster was what one group called the 'payment' ones: ACC, WINZ and IRD. Some (Group 3, 4 8) added Housing to this list. Another cluster was 'enforcement' agencies: Police, Courts, Immigration.

Some groups (e.g. 2 ,4, 5) included a large number of agencies in their comfortable group because they did not have much to do with those agencies and therefore those agencies would have little or no private information about them to share.

A number of groups were very uncomfortable about information being shared between CYFS and Police (e.g. Groups 7, 10) and illustrated their reasons from experience. Group 7 were very uncomfortable with sharing between the agencies that were required to ration eligibility, and require payments, for example WINZ, Housing, ACC, IRD, MSD, Courts. These were agencies that could make decisions which could have an adverse effect on family income.

Interacting with government agencies such as IRD or Studylink online appeared to remove some of the frustration of providing the same information over and over again [Group 3]. With the provision of user-name and log-in password individuals have secure access to their own information and can make changes to their own personal information.

Generalised distrust of government agencies and negative service experiences by individuals were associated with Māori having non specific reservations about information sharing between government agencies.

> I'm not in favour of them all joining together and sharing information. I'd rather have them separate identities. [55]
>
> I think just keep it separate, because everything will then run efficiently, and be less mistakes. You'll have WINZ people trying to do IRD jobs and things like that. [56]

Cross-government information sharing

Participants' responses to questioning about which government organisations share information now, revealed that a number of participants believed that there is currently a widespread practice of sharing information across government organisational boundaries.

> All government agencies are shared together. [15]

The cross-organisational information sharing referred to included depersonalised statistics e.g. across police, fire, ambulance [13], income and payment information between the 'paying' ones such as WINZ, ACC and IRD [3], and also information about individual clients e.g. WINZ and IRD [13]. WINZ and ACC clients were aware that there is some sharing of information now between these agencies although there appeared to be a low level of understanding about the form this takes and why something already known by one agency is not known in the other.

Some also understood the conditions under which this information is shared and are permissive provided that they are advised in advance that the information will be shared and the purpose for which it will be used. They would however like to be convinced that there are benefits for them personally from information sharing.

> We don't like unnecessary intrusion into our personal affairs. [27, 28]

Some had experienced information sharing used for monitoring and compliance purposes at close quarters, such as Courts fine information with Immigration, and IRD and WINZ.

> Mate got caught … he was working when he was getting a benefit. [1]

> It happened to me … my wife was on sickness benefit, she had $100. Because I run her business and I can raise my pay anytime I like, I raise myself and all of a sudden her benefit came down to $13 a week. They might know that I raised my pay so they drop sickness benefit. [2]

Monitoring activities loom large in some people's experience

> If you owe money to the Inland Revenue they can contact your Bank and take the money out. They can – if you owe a big amount, and they want it –they can take it, and you've not got no say in it. [62]

Young people were generally permissive about information sharing between government agencies.

> I don't really mind (sharing). I assume the government agencies are going to share information. I also assume that they are going to know what they are doing. [13]

> Some people might feel uncomfortable with the facts that are shared, but I don't really – I think some people would complain about it, but that's probably people trying to beat the system. [36]

Discomfort with information sharing between agencies by ICT savvy users such as students was linked by them to a lack of knowledge about specific government organisations and what they did, and therefore their reluctance to have these organisations share.

> I'm not happy giving people trading information if we don't actually know who they are and what they do. [15]

Non-users are also aware that information sharing and information matching takes place between agencies for clients in receipt of specific services.

> It's actually written on – it says that this information – may be used with – it's Inland Revenue and WINZ work in together, and they share information at any time. [61]

> I went to a seminar at WINZ just at the end of last year and Inland Revenue were there and they were there for us to ask them any question we wanted to. They told us then that you try to go out of the country and you owe X amount of dollars for child support, you can't get out of the country. [61]

Both the Māori and Pacific groups were more suspicious about the need for providing information and less trusting about how government organisations will manage this information. There is no significant difference between the younger and older Pasifika participants in this respect.

> I'm very hesitant. I just don't like leaving anything where somebody can pick it up, even though it is modern technology and you should move with the times, I'm still very reluctant. I don't even feel comfortable on Facebook. [45]

> I don't have a problem (with providing information). No, I think it's a part of their processes and I do trust people. You've got to trust people. I give my information out. The only thing I don't give back is bank details – I don't mind giving my bank account details if they're going to deposit money into my account. [55]

> I don't like to give my children's details out. [55]

> I don't really have an issue with if I'm filling out forms and giving out information – I don't mind giving out information, but I will stop at giving my bank card number. [58]

To Māori, the information asked for is sometimes out of proportion to the services that are sought.

> If I'm just making an enquiry and they want all of this other information, when I'm just making a general enquiry – I get really annoyed at government departments when you have to give your name, address etc.. All I want to know – now, who do I contact? … It's like they want to check on you before – but it's just a general question. … So, why can't they just have a call centre type thing for general things, where you're just asking on a general level. Then, when you want to go in to get something more official, then give all that information. [54]

Pasifika felt powerless about the sharing and management of personal information across agencies.

> They've got all the information that they share out anyway so we really feel…we can't do anything about it. [50]

If they had a choice, the Pasifika group would rather that there was no sharing between agencies.

> If we had a choice, I don't think we'd feel comfortable with sharing anything. [49]

> For me – knowing that somebody else in another department knows what I'm doing or how … is a bit uncomfortable for me. [48]

Some participants held specific views on when information sharing should be further promoted.

> ACC and IRD should be working a bit more together because people who go on ACC come back and work partial hours aren't told that their ACC earnings should be a secondary tax and their employer

> ends up paying so therefore they are getting pinged at the end for each extra tax – it would save a bit of work at the end of the financial year. [9]

> Why isn't the government one tree instead of half a dozen bushes! – IRD and WINZ could be the same department easily. [8]

The desirability of more sharing between Immigration and IRD, and Immigration and Courts was also mentioned in this context. [8]

Implications of information sharing

Participants expressed general support for information sharing between government departments 'depending on what it is used for' [3] and 'provided it is used for the purpose it is meant for' [1]

> If you are not breaking the law, it shouldn't be a problem [7].

Most participants saw benefits in the sharing of statistical information for planning purposes and informing the public. They saw this as helping the agencies to do their job properly, to develop new policies and services, and to be able to provide the right services in the right places.

Participants wanted to be convinced of the benefits of more information sharing to them personally.

> It's also the question of how much information…. Like you would like to tell IRD certain information but you don't want others to know about. So its like if they start sharing information and it gets out probably don't want to … like if it's a contractor who is working or something in another Department you wouldn't want to know income or financial strength [1]

They saw it as stopping people from taking money they are not entitled to and also avoiding the information loss problems encountered when a client is passed from officer to officer within one agency or between agencies.

Information sharing is seen as one way in which government agencies might be able to do a better job for clients with high and complex needs.

> If you've got somebody who's applying for a benefit – they've been kicked off ACC because ACC don't want them there – so they've got to go and get a sickness benefit. You have to contact ACC to get information for that benefit. They'd also ring Housing New Zealand because he's got three kids and lost his job and Housing has given him a job. So, you have to link all up. So, just by using the telephone to make sure that you do get the right information – that the person is going to get the correct rate of pay, you should be able to link up and make a phone call – case manager to case manager – and then they get the information, and it's accurate. [52]

Younger participants saw advantages to information sharing between agencies such as ensuring individuals get the right entitlements. They also saw advantages to individual agencies focused on particular services, allowing them to plan. They were cautious however about the over-categorisation of individuals.

> I think they should be able to share the relevant and necessary information, its still good having an independent side to it because then they can actually focus on what they are trying to do instead of again just generally categorising in a box because you ticked four boxes instead of five [1]

Group 1 discussed sharing of information between WINZ, CYF and Housing NZ because 'there is a lot of personal stuff that have the power to make or break peoples lives' [3]. In the group's view, what information can and should be shared 'depends on the information'. These agencies they said 'have a lot of power over peoples lives, housing, make up of families, the amount of income that you are bringing in – they are giving you benefits. They can make your life easier or they can make it substantially harder' [5]. There was concern expressed about the accuracy of the information being used and its current relevance, especially when this information is being used to categorise clients and determine eligibility for services 'if they put you in the wrong box and you get a case manager who doesn't like you or you don't get on with them, it can make things really, really hard' [5]. There was a concern that relevant information might not be asked for, such as not just number of children and their ages, but also the extent of their dependency, for example a case where a child is handicapped in some way and therefore more dependent.

Young people see information they provide to government agencies as part of a reciprocal trade in return for services they want and therefore they make a judgement about what it is reasonable to provide and what is not.

> I don't mind because – in the case of Studylink at least – the details that you are giving them is probably in the long term helping you…. I would only have a problem with it … if Studylink wanted to know if I had any convictions, because that's not really to do with whether they give me a student allowance or not. [14]

Participants saw advantages to individuals and to the collective interests of country as a whole, from government organisations working together and sharing information.

> The reasons for swapping are to keep it easier. [21]

> I don't see any downside as long as you play the game. If you have nothing to hide, I don't really see it as an issue. [20]

> The advantage was that with shared information, hopefully will save money and time. [46]

Examples given included sharing between IRD and ACC to assist people who have been on ACC when they re-enter the workforce on partial hours. WINZ and IRD should also work this way [12], and Courts [11,9] for the recovery of fines to avoid the individual having to provide proof of earnings to Courts.

> If Courts worked with IRD, they could find out where somebody is being employed … send it straight on to the employer to get deductions made … it just cuts a bit of time [9]

Participant's attitudes to information sharing across government organisational boundaries took into account the closeness of the mandates and the overlapping responsibilities of agencies. Where mandates or responsibilities were perceived as close or related (for example, Justice, Courts and Police or WINZ and Housing) then groups tended to view sharing between these agencies as OK. This is because participants thought the agencies would be able to help each other and could do a better job if they shared [Group 8 and 10].

> We've just kind of split all the government departments into basically three areas: One's with all the Police and Court and everything; one that mainly deals with income, like the ACC and Work and Income and so forth; and then the other's that don't have anything to do with us, which is the Ministry of Fisheries and Agriculture, or only if something pops us and the more that had to do with

> our own development, like education and health and that, most of us felt comfortable with them sharing information but the other's we're really just split. [49]

Information sharing for monitoring eligibility and compliance were more contentious. Many knew about the justice sector initiative to monitor those leaving the country for unpaid fines and prevent people from leaving until fines are paid. This example was part of a scenario put to the focus groups and is discussed in another part of this report. Few expressed any objection to this practice and saw it as generally fair to all.

Employed wage and salary earners in the South Island saw advantages to regular surveying of employers and links with Immigration as well as Courts, WINZ, IRD, and ACC mentioned above [e.g. 24].

One group of non-users in a major North Island centre [57, 59, 60, 61, 62, 63] had only three agencies they were uncomfortable with sharing – NZ Police, CYF and WINZ. Their reasons for this were that this sharing often led to false accusations being made about individuals.

> At the end of the year, when you are paying your tax, receiving any benefits or anything, everything will be working and you are not paying too much, not having to pay anything back, don't have a bill at the end of the year [9]

Māori, Pasifika and some North Island minor centres were less supportive of this view. The advantages were seen as the individuals getting the right entitlements and avoiding the discovery of overpayments that need to be repaid at some point in the future.

NZ Post was named as an organisation that passes information to other agencies as part of the change of address form people fill in, provided individuals give permission which might be done accidentally. [10]

Some had experience of information being shared about tax paid on savings and PIE investments with banks and other financial organisations managing these investments on behalf of their clients. This was seen as beneficial to the tax payer, ensuring that they were taxed at the right rate and were not left with additional tax owing.

When participants discussed the agencies they were uncomfortable about sharing information (see Table 11), the answers fell into two broad groups: (a) agencies whose mandate and functions were outside the experiences of the participants or unknown to participants. In the absence of knowledge about what the organisation did, what information it might use and how this might affect individuals, participants were generally uncomfortable with sharing information with these agencies and having these agencies share information with other agencies they did know; (b) agencies with a monitoring function and powers to force compliance such as Police, Agriculture and Fisheries, Customs, Immigration. Occasionally, one of the service agencies, such as Education or Health, featured in the uncomfortable list because of the negative experiences of one or more members of a group.

> Police rang me about someone who had defrauded us and they were working on the case and said, by the way, your registration is due on the car [22]

Groups 2 and 4, and also some others, brought a taxpayer view to the benefits of sharing information. They particularly perceived the benefit of a fair allocation of taxpayer funded services.

> The advantage was that with shared information, hopefully will save money in time. [46]

Participants also referred to statistical information gathered from service delivery sources being used to improve service quality.

> I personally like giving stats, because I think we are looking at improving nationally where we're at. You know, how many of us are employed, how many Māori are out there working, you know, what are the stats with our refugees coming into the country – I don't mind, because I think it helps with things like (what services are needed). [52]

Examples of information sharing that groups thought are desirable for the benefits it would have to the wider community were discussed, for example Transport NZ providing Police with information about driver licensing and vehicle registrations.

> You'd like to think that Police would have that information any way … as far as Police doing their job and keeping the community safer and a better place, you'd like nothing better than information be readily available. [20]

4.2.5 Information privacy

Participants were probed for their attitudes to informational privacy and what information in particular they considered private. Context was an important feature of participant's responses.

> It depends on who I am giving [the information] to … I am more likely to give my bank details to Studylink than to someone who asked for them on the street … basically you assess the situation. [14]

> I do like electronic, but it depends on what it's for, and depends on how much [information is required] – Not a hell of a lot I don't think – not when it's got all that stuff on there. I mean, you have to give your IRD number and things like that. If it's just general name, address, date of birth – just for confirmation – that sort of thing I don't have a problem with. [54]

Groups 4, 5 and 7 held strong views that all personal information was private and they share it with government agencies reluctantly and only if they have to.

Financial affairs were widely considered personal irrespective of age and income level.

> Your income is pretty personal … debt as well. [14]

> We wouldn't just hand out all our detail. It's the relevancy thing [36]

> I am happy to provide generic information, but when it comes to things like salary … I think that's quite personal. [46]

Participants also held the view that privacy is changing in the context of the general online environment.

> Most people have given the information out so much that it is not like they are losing their privacy…. The reality is that people are going to be able to find out information about you if they want to … like anyone has Facebook these days. [13]

There were no consistent other patterns about what is considered private – the context appears to determine this. Some considered date of birth private if it is used to categorise the person; even

address is private information when the participant does not want to give information about where they live.

It was common across all age groups that what is considered private depends on the circumstances and the benefit to the client in supplying the information should be readily apparent.

> Well, it depends what you're getting out of it. If you're in an accident or something, you've got to give information. If they're going to pay compensation or something like that, or if you go into hospital, you've got to get a certain drug. So, you've got to give them information on that because they don't know what they're to give you. Stuff like that benefits us. It's stuff that you know benefits yourself, but a lot of other stuff are just clap trappers. You've just got to ignore it. You get no value out of it. [25]

One Pasifika participant commented that people are reluctant to provide private information in circumstances where it is not understood why the information is needed and what the information is going to be used for. These sentiments were echoed in various ways in the Groups 5, 7 8, 9 and 10.

> When people think it's too personal, it's only because they haven't been told why they (the government agency) need the information. [49]

Individuals tended to regard information that could be used against them, or information that might lead to a misjudgement of what the individual viewed as their own vulnerable circumstances as private.

> Some of the questions that they ask you are actually used against you … they take information and they penalise you with it. [42]

> That could not go in our favour sometimes … and sometimes you don't have a say about something that we think might be unrealistic. [59]

Perceptions of privacy among the participants were related not just to the information being provided but also how it was being provided and under what circumstances. Super-annuitants (65 years and over), participants on benefits, and other high users of government services tended to think they were being asked for too much private information. They also felt that they did not have any choice about providing the information asked for because they needed the services to survive.

Younger people saw concepts of privacy changing with the e-service environment and the technology.

> Five years ago you wouldn't have said that – it makes you wonder what will be acceptable in five years time? [17]

The younger users also saw privacy as a relative concept in the context of what is already available publicly through online sources.

> I could look at all your photos on Facebook if I wanted to, and I know your name now. I could go home and jump on Facebook … I've got your face I know all your friends. [15]

The older group had a strong sense of privacy and were not happy about the amount of information they are expected to provide.

> Our age group – we're not used to telling everybody everything about ourselves. [30]

> There's always something they want to know about your past life. [26]

As you get older you have to give out more information too. [25]

It amazes me because they get all this information and when you ring up and try and find something out, (you) go through about six different phone calls before you get something. (Then) they say they'll get back to you, and two weeks later you ring up again to find out what's gone on with the information that I wanted. [25]

4.2.6 Trust in the e-service environment: information security

Security of information and the security of transactions are part of participants' trust in the e-environment. There are linkages with trust in government and government agencies (please see 4.2.3).

Participants made judgements about which organisations and services to trust on a case-by-case basis depending on circumstances. Size and reputation can be factors influencing this choice. Sometimes there is an element of 'no choice', namely the next best option, such as no service at all, is even more unacceptable.

I do quite a lot of Internet banking, and I trust [35]

You trust all the big companies … when we lived at the flat, you'd have to pay the power bill – like we'd give the credit card number and just trust that they'll pay the bill [34]

Peoples' awareness of information security issues is linked to their awareness of the e-environment. Across nearly all the groups, participants illustrated their attitudes to online security with anecdotes about Facebook and other social networking tools, and the use of online banking.

The trouble is with that they think that it's private and its not. It's like a postcard.

Like they are telling people not to put your age, you know your name and your age you're prone for run-ins…. I have a security background and one of my mates was always telling his wife not to put information about their kids on Facebook – it's just like anyone can read it. Something that you need to be worry of I suppose [18].

The point was made that so-called security measures are not always easy to use.

Those human testing things [the visual confirmation words that some websites use to verify that a human is inputting the data to avoid spammers] – we have to type in the word. I hate that. Half the time I have to reset it because you can't actually see it to do it [32].

Even non-users were aware of online security issues, mainly from what appears in media or through anecdotes.

How would you know if anyone was hacking in and finding out your details? I mean they do do it…. they hack out what you're doing. So they might have all your details and know all your personal stuff?... I wouldn't even do money transactions either. [61]

Younger participants and high users tended to the view that trust in the online environment is transferable.

If you don't trust it for one thing, then don't trust it' and 'if you trust it for one thing, then there is no point in not trusting it for another'[18].

Information security is not limited to the online environment and can also relate to the paper records. For the majority of participants, traditional paper-based and face-to-face transactions were a feature of their recent experience. The perceived security risks of online transactions were noted by several participants.

> It may come to light that it might be alright to do it online, but it's just the fact that when you are online everything is open basically for everyone to see that goes online. Whereas, if you fill out a form and send it away, it's going to get to the government department, in most cases that you are sending it to. [24]

However, it was recognised that the traditional forms of interaction could also be insecure.

> The biggest joke is that while we are talking about all this online – if I need somebody's details I just go up to their letter box and take out their bank statements!
>
> … Exactly, or the rubbish bins! I can't see online as any more unsafe as doing that. [18]

To a certain extent some people trust that what they do online with a government agency is secure because it is a government agency.

> Should be reliable, shouldn't they, government departments? … I couldn't imagine that you could ever be 100% sure. [30]

Perceptions of security risks affected participants' avoidance of online channels.

> You have to have guarantee from whoever running the Internet that it could not be hacked into. [25]
>
> The information might be ... can be, taken ... somebody can break into your computer and get your information. [39]
>
> With form filling-out online for a government department, when … it's sent you don't know that it's going to that particular government department. You don't know where its going to before it gets there. Whereas when you post it, it goes to a specific address…. [Online], the moment you press the button or cell phone it's digital. It's out there in the ether and anybody can hook on to it if they've got the right equipment. So … post your stuff in, it's only the mail room that can play with it, on its way through, so that's a consideration too.

Some focus groups discussed how they decide which online information to trust. Some of the younger participants singled out the government agency domain name '.govt.nz' as a trusted brand believing it to be licensed, monitored, and more difficult to fake than '.co.nz' or '.com'. [16, 17].

Internet users made sophisticated judgements about when and when not to share private information. The context in which they are asked for the information affects their perceptions of online security.

> If there was an official page – I was on the Studylink website – and it asked for my bank details and it was the right situation I would put them in. But if the Studylink person rings me up on the phone and said we just need to confirm your number, what is it? I wouldn't want to give it to them. [15]

Several groups had discussions about what gives them confidence in agencies to manage their personal information securely. Mostly this confidence was shaped by personal experiences. There was a tendency to trust government agencies to keep private information secure without there being any specific knowledge of how they might do this.

> As long as they keep it secure we have nothing to hide…. I worked for Government all my career and we're just not that cunning and nasty and smart. Pretty harmless government – and pretty uncorrupted. [6]

Trust in the e-service environment was also affected by stories people have seen in the news media. One example included the deliberate release of private information by individual staff acting illegally. Doubts and suspicions about the integrity of government agencies and their staff were particularly common among participants from the beneficiaries group, Pasifika, Māori, and non-users.

Providing personal information over the phone was compared with providing it through the Internet. One participant observed that information provided over the Internet

> …travels further because there are more points at which it can be intercepted over the Internet than if you are just filling out a form [13].

High Internet user participants were concerned that insecure personal information could lead to identification of an individual person, although they did not see this issue as limited to government agency transactions. They expressed concerns about identity theft.

> Well you'd like to think it goes to the right person, they see it and that's it, stored away….

> We are transferring our ID and if you know about identity theft… You know if there's a hole in their computer and somebody can get it, all of our names and all of our details then suddenly and our birth certificates suddenly [18]

> A couple of years ago my supervisor he started looking after celebrities and seeing what their incomes are and stuff like that. They've obviously cracked down on that but it was quite prevalent for a while. Which means that anyone could be looking up their information, if they work with the IRD, just to check out. [22]

Asked what would have them trust and use online more for dealing with government, participants focused on security and ease of use.

> It would need to have really high security measures, but you'd only need to do it once [32].

> Centralise….Make it one login [37] One log-in for all [35]. You'd lose that whole thing of forgetting your password for it. You'd only have to do that setting up security verification thing once, and hopefully you'd use it enough that it would be naturalised like Internet banking [32]. It would be good to be just be able to login under one government thing, or send branches off to others – like while I'm here I'll do blah blah blah – and just click on the link there, seeing the link's already logged in. You don't have to worry about going through it all again [34].

Some participants saw the online channel as more secure than offline channels

> People are quite afraid but for good reason…. If I was on the Studylink website and it asked for my bank details – if it was the right situation, I'd put it in. But if someone rang me and said they were Studylink and says they just want to confirm my bank number, I wouldn't give it. [15]

Concerns about information security often focused on human error at the hands of officials within government agencies. These errors were perceived to be caused by carelessness, neglect or omission.

> If you send it in by paper on a form and then they computerise it and send it out isn't it out there anyway, can't people pinch it anyway? Just means you've got a copy of what you sent [18]

> If somebody has taken our identity through somebody else's irresponsibility then they should be held accountable, there should be some come back…. I don't think there is nothing the government can do to stop it, because the security is not there and I don't think it ever will be there [18]

> I think people make mistakes. Human! It doesn't matter what department you work in or where you are or whatever you are doing, if there is a human element involved there will be mistakes … but some agencies have a culture of mistakes ... [example given] Total incompetence. There was a whole culture of incompetence [18]

There were also concerns expressed that too many people have access to the information individuals provide to government departments and that there are inadequate processes for managing its security.

> There's too many having access and I don't think they have enough process in place at the right levels. [54]

Information accuracy

One aspect is the accuracy of the information – the means by which information accuracy is assured, and information remains current. Participants were aware that the information they provided to government agencies is stored against their name, might be used for further interactions with public sector agencies, and might endure for some time making its accuracy an issue.

> If somebody slips up inputting that information in about a particular individual they might get some people mixed up and there might be some information in there under your name that you don't even know is there, which suddenly pops up somewhere and may affect an application in doing something. [24]

> That's what you do if you are talking to the IRD they always ask you if you are at the same address, check that, yes you are or no you are not, they would have access to all of that because if that was one number they would have up to date employment details as it would all be going through one number [9].

> You hear about people, when they've had identity theft, and they've had it so hard to try and get out of that – but see, the other people who have got their name and their details, they can carry on, and the one it effects have a hell of a job trying to prove that they didn't do what this person's doing. So, where they heck did they get the information from? [54]

Some groups, for instance Māori, were particularly sceptical about the misuse of their information that is possible once it has been provided and is stored by government departments. This related to distrust in organisational processes to protect data from misuse and human error or misdeeds.

> We shouldn't have frontline staff able to gather information about people. They're human – they'll gossip. [52]

> I don't mind my information being there – it's who's using it for what, apart from the purpose I gave it for. You've got no control once they've got it, and even if they've got this process in place, and it's legal or not legal, it doesn't stop other ones accessing it. [56]

Participants were concerned that they are not able to see the information held by agencies about them and check it for accuracy. This is also referred to as the lack of control over personal information, which is further described under the analytical theme 'transparency' (please see section 4.2.9).

High users know that the security of their information depends in part on the systems operated by the receiving organisation to hold it securely.

> If you put in your details, and press send, it's in their hands – they can do with it what they want. You give it to them on the phone, it's in their hands – they can do with it what they want. Once you have given it, no matter whether it's online or phone, it's in their hands. So really the security of it is in their hands and there is nothing you can do about it. You kind of just trust that if you do it online the system would be relatively safe at their end. [14]

People with hard to spell or long names find that entering their own information over the Internet has the benefit that their name is spelt correctly, always.

> It makes it easy for someone like me with names that, if I say them on the phone, no one knows how to spell it.

Filling in forms yourself is seen as less subject to human error.

> You are putting it in so you know that there is not going to be human error at their end. [8]

> [Government agencies] have a lot of power over peoples lives – housing, make up of families, the amount of income that you are bringing in, they are giving you benefits. They can make your life easier or they can make it substantially harder. I'd say some of that is up to you but if they put you in the wrong box and you get a case manager who doesn't like you, or you don't get on with them, it can make things really hard. [5]

There was recognition that good services delivery depends on up-to-date information which the client has to provide. However, there was also a perception that agencies might not actively support this, as they do not ask clients to update their personal information.

> When you fill out any form with Work and Income, you've got a form at the back that says you've got obligations to advise of change. I know Housing New Zealand do the same. Land Transport do it too, because I've just had to fill out all my new details. So, we (agencies) will find these things out, if we go in and tell them – if they send out a form to update your details. Otherwise, we probably don't. [52]

4.2.7 Awareness

We observed three different areas of awareness among participants:

- Technological awareness - Awareness of how the Internet works and the attendant benefits and risks.
- Administrative awareness - Awareness of how government works, particularly its legal and administrative procedures for protection of the individual (e.g. the Privacy Act, 1993), delivering value for taxpayers' money and public accountability.
- Service awareness - Awareness of the services available to individuals, how these might be accessed, and the reciprocal responsibilities involved.

These are discussed in turn.

Technological awareness

Technological awareness, across the groups and between individual participants, ranges from a higher level of awareness to a practical and detailed understanding of how the Internet works and what happens to information transmitted through the Internet. For example, whereas Internet non-users displayed some understanding of how the Internet works and how information that is supplied electronically, is transmitted, stored, and can be vulnerable, younger participants showed detailed understanding of the benefits and risks, including security risks, involved with the sharing of information via the Internet.

> As soon as that goes past, not as secure as well, and anyone can get their hands on your identity I suppose. [1]

> Because with online … there is a number of … programmes and different things you can put on your computer. There is a special lock thing on your window and you can tell if the sites secure. I guess you are not 100% sure but at least you feel like it safer. [14]

Participants' knowledge of technology appeared to be influenced to some extent by stories people had picked up from the news media. The effect of this information on high Internet users was filtered through their own experience, while low and non-users tended to dwell more on stories which reported some harm occurring to the individual because of the use of technology. Non-users and low users spoke about an 'over-reliance on computers' and the ease with which a web site might be 'faked'.

High users, aware of security issues, still considered Internet transactions as preferable.

> It's almost like the systems are not as secure as, but that's the thing, it's better than - I think its better than – getting paper stuff. [1]

All high users and those with experience of a number of online services, such as Student Loans, Working for Families Tax Credits and Child Support, understood how the system automatically checks for information completeness.

> Some of the forms are like that now. You fill in as you go, but if you don't answer the last question and skip, it won't let you go to the next question – after a while it tells you… your form can't be completed unless this is answered. [49]

Non-users also had awareness of online privacy and security issues, mostly informed by media reports, rather than hands-on experience.

> The only thing about online is….I think it can be quite disastrous if you make the wrong move – it's so vast – so worldwide. Whereas if you just fill out a form and do something… it's probably more confidential, more private, more safe, because you've got Privacy Acts. So you can actually say to someone – that's not going to be used for such and such, or that's not going to go to this or that… They should be able to say that… but of course you can't do that online – with Facebook and Bebo and all that sort of stuff. [59]

Administrative awareness

Administrative awareness varied. It was higher in some groups, such as main centre participants, people in employment, people in receipt of a number of government services (for example, beneficiaries), or people currently or in recent times employed by government agencies.

> I think they would probably give you information, wouldn't they? It used to be that you didn't even know what the doctor had written up about you, but now everyone can go to the doctor and find out everything they have written about you. [3]

> At least if you are logging on to an organisation or government department you only need your details once and then you can just go in and do what you need to do. [5]

> I think most government departments anyway have policies and procedures in place where they have to do some kind of regular check – whether you're still at the same address, whether you're still the same person. I've had that in the past where I've had something arrive in the mail to say – especially with the electoral roll – please correct your details, or are your details correct. You don't have to send it back if they're correct, but if it needs to be changed, like an address or something, then you've got to send them back that. [55]

Some people were aware only in a general way that there is some legal protection for their private information.

> There's a privacy thing that you've got to abide by. If you break that then you've broken the law – so people you might be in cahoots with – it's done illegally. [58]

Six of the ten groups talked specifically about the Privacy Act, its provision and requirements, in an informed way. This tended to be led by people who had some experience of it, or had worked for a government agency at some time.

> It's a confidentiality thing. You work there, you sign a confidentiality clause. You breach that – you pay the consequences. [9]

> I think with the code – with the new privacy commission – I very much doubt that would be happening, because of the Privacy Act. Since it's been in, my understanding is that you can't give other information to another government department. [52]

Some Māori participants demonstrated their administrative awareness around information privacy.

> Most government departments, you've got to sign a declaration. You've got to sign a declaration to say that you won't give out information – that comes under the privacy act. Once you've signed that declaration, you've got to abide by it. [58]

The Pasifika group showed administrative awareness of the Privacy Act, 1993, and its implications for information sharing

> They need permission to release – I think when you fill in the form you sign that authority away anyway – but I would feel more comfortable if they were to send me a letter saying… look, so and so's asking information that we have on you and we want to release it. [49]

The older group were also aware of administrative and legal provisions, such as the Privacy Act, 1993 and the steps expected of employers to make sure employees understand their obligations to keep information private.

> A lot of places, employees are meant to – do sign an agreement where they're not going to divulge personal information, and I think sometimes that the trust is broken, because we see the result of it in the courts. [30]

Personal experience of privacy and information security procedures, especially from people who work in government agencies, provided another perspective.

> You will have people out there who will (breach privacy), but I know for a fact that we have – we are foot-printed. Nobody can go in and access somebody else's information. You can't even go and look. [52]

Service awareness

Service awareness was illustrated through participant's experience of government services, their insights into how well these services work from the client or taxpayer perspective, and the impact that service experiences have on future use. This has some overlap with the analytical theme of experience, skills and ease of use (please see 4.2.8).

Service awareness was high among participants who are consumers of a range of government services, for example the beneficiary group. It was also common among the Pasifika participants: like many other groups Pasifika would like government agencies to be more transparent about why they want to know certain information and the implications of providing that information.

> When you first ring the IRD, they always ask your IRD number. If you don't have one then they just flick you off…and then go…and get you one. If you don't have an IRD number, then you're helpless sort of thing. [50]

Younger participants displayed a lower level of service awareness compared to other participants. They had low levels of understanding about government, its agencies and how they work, with the exception of Studylink, that most had dealt with. Their lack of experience translated into trust of government agencies and their service provision.

> It's never gone wrong for me so you don't have any reason to be suspicious. [13]

In general, service awareness involves knowledge of the reciprocal exchanges of personal information for services from government agencies. Information is provided by clients to:

> Assess the decision they are trying to make. [10]

Sometimes the information exchanges are considered burdensome and provision of information by participants becomes more resented.

> Or hope they'd stop bothering you [laughter] by providing them with the information they are looking for. [10]

4.2.8 Experience, skills and ease of use

Experiences affect peoples' attitudes to a service and to the agency providing it.

> You quite often pick up straight away on the telephone whether you're going to have a bad day or a good day with the person you're talking to … that first ... how they describe themselves over the telephone ... this is [name] or whatever it is, from Inland Revenue, how's your day been or whatever. That's going to be a nice conversation. [39]

First experiences can shape future attitudes to a channel and a particular service for the longer term. Positive experiences generate repeated use.

> I got fast tracked... and it made things a lot easier and because I only went into one place, you know... it was all online ... it was a lot simpler and after all the hassle of getting on the benefit and moving cities and all that hooha it was, yes it was very good. [43]

Frustrating and bad experiences deter future use.

> You click on … whatever it is and it takes you so long to get it and there is so much other information to do with the same form that you sort of get bamboozled. [10]

The attraction non-users have to the face-to-face channel is partly influenced by their experience of other channels.

> I don't think they'd all be talking to you as nicely and as friendly if we were on the phone to you but because we're talking to you face-to-face we can gauge your reaction, we can see how you're responding to us.[42]

Several participants told of frustrating experiences they had trying to access a number of different government services, which tend to make them less inclined to try again. IRD, joining and changing Kiwisaver accounts, and Working for families Tax Credits were three service areas that were mentioned more than once [52, 54]. They focused on aspects like too much information or badly organised information.

> You click on WINZ or whatever it is and it takes you so long to get it and there is so much other information to do with the same form that you sort of get bamboozled. It's not just the form. It's that sort of that part of the form on one page and go through the website to get a little bit more…. For me if the online service was more ideal, simpler [10]

> I'm an extramural student so I go online all the time. I applied for a student loan because I'm a student and it was all done online… It's a lot more work than I thought it would be…. Having broadband has really helped because you know, waiting around is just, if you do something slightly wrong, and that it just all freezes up .... argh! [43]

Participants had expectations that government agencies would be clear about what they can and cannot do, and would stick to their word. The examples of participants' experience where this is borne out in practice, were few compared with the number of accounts participants gave of non-delivery on promises.

> If you ring the IRD … if you were to ring them now... and you couldn't get through … you actually leave your name, your tax number …. and they say your call will be returned to you within 15-20 minutes and you can guarantee that within that timeframe, you've got your call-back. So you don't go on thinking, if I go out they're going to ring … or something…. I actually said to them on the phone… I'm very impressed with your service because you have returned my call…. because I like my calls to be returned if it's something really important. [62]

Ease of use

An easy-to-use system creates satisfied clients.

> I did [my tax return] online and they just sent me a letter saying how much it was for and a cheque for like $70 – but yeah, I did it all online. [34]

A frequently mentioned technology encountered when dealing with government and non-government organisations is automated telephone response systems. These were generally not regarded favourably and were a source of irritation and frustration to those who have experiences of them.

> Another thing is, some of the recorded messages. I'll give you an example for WINZ – if you don't say the right thing, it will say "oh, okay, hang on, I will pass you on to somebody". This is after you've said about 3 or 4 times. [59]

Experienced e-channel users appreciate the convenience, speed and immediate availability of their information.

> You can actually have a log in with IRD so you can get your earnings information from IRD yourself, can actually register … I like it because I can access my own information so I can see how much I earn each month, each year going back … because of the nature of my job I can work out how much, what my tax position is end of each year and know how much family support I'll get …. And its always good if you can just do that without speaking to anybody. You can do it privately yourself without questions and take in, read the relevant information, take it in and think oh yeah, and then if you have to do anything then you can make a phone call [9]

> Most basic forms you can get them quite easily, and that also goes for PDF files on instructions for specific things, particularly for IRD. You can download PDF files with instructions all about GST, instructions about all sorts of different things, and sometimes its better to download that and read through it which might answer your question and don't have to talk to someone. [24]

> If you get half way through and realise you don't have a piece of information, you can get up and grab it. That's not as easy in the phone. [3]

Log-in and security processes can be off-putting to users.

> Having said that – logging in is a real nightmare. Oh, they get you to like, you know your password has to have four letters and so many capitals and then it says like what's the fourth letter of your pass phrase, and it's not allowed to have certain things in it.[32]

> I tried the IRD tax refund and stuff like that and always found ultimately you have to ring them for some information. [32]

> There are communication barriers around the security systems operated by some departments which deter some users [32, 36].

> Those human testing things [the visual confirmation words that some websites use to verify that a human is inputting the data to avoid spammers] – we have to type in the word. I hate that. Half the time I have to reset it because you can't actually see it to do it [32].

The younger participants (under 30) had a broader knowledge and a more positive acceptance of e-services based on their experience of social networking tools, commercial e-transactions (e.g. Internet banking), and government online transactions, such as student loan applications through Studylink.

Child support payers and receivers, Kiwisaver members, Working for Families Tax Credits (WFFTC) and student loan clients are common in Internet user and non-user groups. Personal experience of these services, whether accessed online, over the phone or face-to-face, tended to bring higher levels of service awareness.

> ACC will ask for it anyway especially if you are doing a claim you are needing to be paid. IRD is going to know your earnings anyway. WINZ are probably going to be asking for it, so that's three of them that are going to find out anyway. [8]

> I had to ring WINZ today and they were able to look up a letter that I received just by asking the date of the letter. There happened to be two on the day but they were able to look at the letter and read exactly what I was talking about, so that was quite helpful. [5]

> That's what so good ring them up, see what forms, you can talk to them about what forms you actually do need to down load, they'll give you the numbers to down-load. [8]

> We go to ACC regarding a client's ACC levies. You can use the IRD number if we don't have an ACC number – you use the IRD number to access the account, so that's already linked. It's already the foremost number. I mean WINZ need your IRD number and you can access everything everyone needs, your employer needs. [8]

People who suddenly find themselves in need of government services find it quite difficult to get the information required to access those services. Service clients have to learn how to get what they need.

> I think a lot of the time it's just lack of training. Nobody really gives you the information that you need. Since I had the accident, I now ask specific questions, rather than asking general questions. [49]

> (Government agencies) don't give out enough information for people who go through them, of what they're entitled to – they've got to find out for themselves … not helpful. [52]

4.2.9 Transparency

Participants generally described feelings of information and process asymmetry in their dealings with government agencies. They don't understand the decision making processes or what services might be available.

> You don't know what they're doing on the other side of the phone. So, it comes down to exactly what you said – you've got to just trust that they're doing the right thing for you – for me, you know? 55]

Participants noted a lack of transparency about what happens to the information people provide to government agencies. A lot of the information provided feels one-way to participants.

> I think it would be nice if there was a little bit more communication and just like a gesture of….we've just done this….or we're just letting you know….so, I think that's nice. [59]

The reasons for providing information are not clear to participants and neither are the conditions under which it will be stored, used or shared.

> I'd just like to know who has got my information. And, if it's going to be passed on, that it will be passed on [23]

> We don't [know what they do with it]. We are trusting them! [18]

There is a definite feeling among the older participants that government agencies do not share the information they have with clients in a transparent way.

> A lot of government places would say they've got their own book of rules. We've got our own laws too – for privacy. Good enough for the goose is good enough for the gander. [26]

> I don't really quite understand … whether they are to protect my privacy, or whether they're poking their nose into my private affairs. [28]

To participants, the standard agency practice of asking for permission to use, store or share information is not effective in making interactions with government agencies transparent.

> The fine print that we don't normally read. [16]

> And jargon that you can't understand [17]

> I pretend that I read it in front of them. [15]

> How do they cross reference it, I mean you could have a John Smith, dozens, how do they know they've got the right one? How do they do it? Do they type in a name, what other information do they give away to get that identity? [23]

> The information they've got is accurate, not necessarily what you provided, because you don't know what they've got, or whether what they've got is accurate. Are they able to collect information outside of what we give government departments? I'm sure they do [24]

> Like does it just get used for its purpose … does the surgeon end up reading this form and then once he's finished with the surgery and he's discharged you, does it just go in the bin or does someone store that information somewhere? [7]

> You'd like to think it goes to the right person – they see it and that's it, stored away….

> You can ring a government department and say I want to sort out an accommodation thing. You don't say it straight away, you say my IRD number, they ask for your IRD number straight away, then you say this, this, and this, [and they say] oh sorry I'll put you through to somebody else. So you've given half your information to that person who is nothing to do with it. Then … you've got to start again and do it all. That first person has got half your information that you didn't need to give to that one person, so what do they do with it? [10]

People generally liked the concept of transparency about the rules and the procedures to be followed by government agencies. This came through very strongly in the discussion of a scenario which involved information about fines owed to the courts in NZ being checked against people departing the country, and not being allowed to leave when there are fines outstanding (See also Section 4.3, Scenario 4).

> I think you should pay. If you can't afford to pay your fines you shouldn't be travelling.

> It's another way to try and just put pressure on people to pay the bills. So at the moment you've got a fine in the court they would tell. And you haven't paid

> They would tell Immigration any way wouldn't they. So it's no different. Fair enough. I think that you can actually pay it right there and then can't you at the airport

People would like to access their own information and have access to check the accuracy of their personal information.

> Maybe we should have more freedom to access things…. to find out proper information rather than getting mislead.[59]

Several focus groups discussed the benefits of a single number or a single log-in for access to government information and services.

> I'd love to know because I'd love to be able to just give a number and never have to repeat it – 'there you go, the information hasn't changed, here's the number, hold on you haven't updated for the last five years so we just might ask you a few more questions, fire away' [9].

> One number – is probably not going to be such a circus [as current multiple arrangements] [9].

> Much less confusing for us [10]

Some participants also saw benefits for them if government agencies had access to the same information and all who needed the information could be updated by a single action.

> That's what you do if you are talking to the IRD. They always ask you if you are at the same address, check that, yes you are or no you are not, they would have access to all of that because if that was one number they would have up to date employment details as it would all be going through one number [9]

> This is the other problem with WINZ not being linked to IRD properly because people get away with it for a period of time, amount of money that they are able to fraud but and if they were comparing information that would put a stop to it a lot faster at least [11].

> The difference, which is not my fault. I put my tax code which is M, I give it to my employer, he puts in the tax code and he does all my tax. End of year they write a letter saying you owe $340, so I have to pay that, but I don't have that $340. Makes it even harder. Then IRD should know that I've been on M for years and years so why can't they know that I'm already on an M [10]

Younger participants expected information and transaction transparency by government agencies.

> I think we should have full access, it's our information at the end of the day. I think we should have access to why they even need all the information as well. If we need to ask that question, why can't they answer it? We are providing it for them to do a service for us or whatever. [1]

> You trust that what they are asking you is purely just a necessity, and the information sticks with them. If you've got nothing to hide what's the problem really – as long as it's not really, really, personal like your account number and PIN. [1]

Participants were also suggesting how agencies could improve their online services in a more transparent way.

> Websites have lots of pages of information that we are not necessarily interested in. Why not have a page that very clearly sets out the information you are providing and how it will be used, where it will go and that sort of thing. [5]

4.3 Scenario Responses

The focus groups were asked to discuss four different scenarios designed to draw out attitudes to information sharing and channel use for particular purposes. The scenarios are recorded here along with a summary of group responses.

4.3.1 Scenario 1

Jacob is divorced from his ex-wife, and has just become unemployed. He is online and needs to apply for an Accommodation Supplement from work and Income. He has to supply information about his children, their relationship to him, their other parent's name, and their age. He also has to supply his IRD number.

Groups were generally happy with this scenario. There were exceptions:

Group 10 (Internet non-users) thought that Jacob should not be doing this online. Instead he should see a case manager face-to-face. Group 9 (Māori) were also not sure about using online in this case.

Group 7 (beneficiaries) had reservations about how much information Jacob should be expected to provide. From their point of view only basic personal information needs to be supplied - *'you want the benefit – you supply!'*

Group 1 (North Island, major centre, salary earners), Group 2 (South Island, minor centre, salary earners), and the females on Group 3 (students) thought that too much information was being sought, in particular providing details about his partner and their relationship was not alright to participants.

4.3.2 Scenario 2

Inland Revenue sends a letter to Janet, letting her know that as she has just turned 65, that she might be eligible for state assistance. However, Janet's partner Jack is very upset when he gets the letter because Janet has recently (in the past three months) died.

All groups agree that this is an unfortunate and sad scenario. All thought that there should be information sharing about birth, deaths and marriages between the Department of Internal Affairs, IRD, and WINZ.

Group 3 (students) went further to make it explicit that information sharing about deaths should NOT include sharing about the cause of death.

4.3.3 Scenario 3

Jocelyn is a university student with a student loan and part time income. She has provided her personal details including her mobile phone number to Studylink. She receives a text message on her mobile phone from IR to remind her that her part time income has fallen below the $16,000 threshold and that she therefore is exempt for the time being in making any repayments to her student loan.

Several groups were not happy with the use of text messaging for the purpose in this scenario. The reasons discussed in the groups included the security mobiles phones and text messages for information that was private to the individual. These groups questioned whether it could be assumed that the text got to the intended recipient (Group 3 – self-employed; Group 3 – Students; Group 2 – South Island, minor centre, salary earners; Group 6 – North Island, minor centre, male salary earners).

Other groups focused less on the privacy or security of the message, and were more concerned in a general way about how it is appropriate for a government agency to communicate about matters such

as this with their clients. Group 10 (Non-users) thought that a letter should be sent or a face-to-face appointment should happen, not text. This view was largely shared by Group 7 (Beneficiaries) and the females from Group 6 (North Island, minor centre, young salary earners) who thought a letter should be sent instead of the text. Group 9 (Pasifika) also thought a text too informal for a department and a letter is needed.

4.3.4 Scenario 4

James is at Auckland airport on his way to Australia, and has a new e-passport which means he can check himself in through Customs and Immigration via SmartGate. SmartGate uses facial recognition software to compare the digitised image on the e-passport microchip to the face of the person at the gate. Other personal information the e-passport's microchip are full name, nationality, birth date, birth place, sex and dates of issue and expiry.

As well as being used by these government agencies to perform the customs and immigration checks that are usually conducted by a Customs officer, James can be targeted for duty free specials on his way back into the country because the duty free shops (via his boarding pass) keep a record of what he bought last time. The system can also tell if he has any outstanding fines to pay before he leaves New Zealand.

No one raised any issues about the use of facial recognition software or the use of the e-passport. Several people in different groups already held e-passports, have used them, and were happy with the process.

All the groups considered sharing of the Courts' information about outstanding fines with Immigration for this purpose is acceptable. "It's fair to everyone – people should pay their fines"; *"If you can afford to travel, you can afford to pay your fines"*.

The majority of groups were not comfortable with sharing information with a commercial entity such as the Duty Free company, and see it as a privacy breach. The exception to this general view was Group 10 (Non-users) who see this as a great service.

5. Meta-analysis of the Research Findings

5.1 Comparing our research participants with other studies

In this section, the demographic characteristics, attitudes and behaviour of the participants in this study are compared with other research conducted in New Zealand and internationally. Statistically valid comparisons cannot be made because our sample of participants is small (N=63) and the focus groups were not selected randomly.

Age

Several international and New Zealand-based studies of Internet use and attitudes to the Internet have identified age as a variable. A Statistics New Zealand survey (2010) identified 25-44 year olds as the highest users. A 2009 New Zealand based survey found an inverse correlation between age and Internet use (Smith, *et al*., 2010).

The Internet use of our younger participants is not consistent with this literature. The younger (18–30) age group in our study were not all high users of the Internet. Proportionally, the 30–64 year olds groups consisted of more high users. Our data is skewed by Group 6, who were low and non-users. In talking about their Internet use, they commented on two things relevant to their low or non-use. Firstly, half the members of the group worked in field jobs or other occupations that did not make computer use part of their daily work life. Secondly, the population size of the centre these young people lived in made face-to-face transactions easier to do because they were known and they liked the social contact these occasions provided.

Our older population (65 years and over) were high users of the Internet in a larger proportion than the other New Zealand studies have found. Only three participants of this group had accessed e-government services, and this was mostly to find information, not to carry out transactions online.

Consistent with the literature (Livingstone & Bober, 2004), our study does show that young people have a different view of privacy. They are more permissive of the use of personal information. They tend to the view that much personal information is already available online and can be accessed by anyone. Therefore, they are quite selective about when and to which organisations they will provide what they consider as very private information, such as bank account details. They expect higher security measures to be in place before they will provide sensitive information.

Older age groups were also aware of the risks to privacy presented by services, such as Facebook, Bebo and LinkedIn. We noted that this awareness was sometimes cited as a reason for non-use of the Internet; however, none of the older age groups identified the Internet as changing the concept of privacy for them.

Gender

A 2009 New Zealand based survey shows that a person's gender plays a lesser role than some other demographic characteristics in determining differences: more or less equal numbers of males and females, just over 80 percent, used the Internet in 2009 (Smith, *et al*., 2010, p. 28).

Similarly, there were 33 males and 30 females in our study and high, low and non-users of the Internet were found in near equal proportions.

Culture

A 2009 New Zealand based survey found that the proportion of Pakeha and Asian people using the Internet was higher than for Māori and Pasifika peoples (Smith, *et al*., 2010).

In this study, all the Māori participants were high users of the Internet. Only two Māori had not used the Internet to access e-government services. Similarly, all bar one of the Pasifika participants in this study were high users and only two had not used the Internet to access e-government services.

Location/Community

A 2009 New Zealand based survey found that Internet usage in New Zealand can be correlated to geographical location as well as size of the local community (Smith, *et al*., 2010).

In this study, six of the focus groups were conducted in the same major centres used in the 2009 study referred to above. However, because the non-user group was recruited from one of these centres, we have a higher proportion of non-users in the major centres. One of our minor centres was approximately only a third of the size of the other minor centres. The size of this centre as well as the occupations of the people in this centre contributed to their lower Internet use.

Level of income

A recent New Zealand-based Survey found that those on lower incomes (under $30,000 p.a.) were significantly lower users of the Internet – for any activities – than those in higher income groupings (State Services Commission, 2010).

In this study, high users of the Internet were found in all income levels in almost equal proportion. Cost was not mentioned as a factor in Internet non-use.

The main reasons offered for non-use of computers and the Internet in this study were preferences for face-to-face interactions and about time use. Older people who were non-users put forward a similar argument: that being online would take time they preferred to spend in other ways.

Education

A 2009 New Zealand based survey found a significant relationship between education level and the predisposition to use the Internet to get information about public services (Smith, *et al*., 2010).

Only a very small proportion of the participants in this study had education qualifications beyond high school level. Because high-school level by far is the dominant qualification in this study, they dominate all categories of e-government use. Consequently, a potential relationship between education level and the predisposition to Internet use could not be further explored in this study.

5.2 Comparing the research findings with theoretical assumptions

In this section we compare the research findings of this study with the theoretical assumptions based on available literature (please see Chapter 3). Under each analytical theme, the following observations can be made:

5.2.1 Individuals' acceptance and use of the Internet

A 2009 New Zealand based survey found that the main reason for Internet non-use was that people did not find using the Internet interesting or useful (42%) (Smith, *et al*., 2010).

Our study confirmed this, especially for our older participants who offered as the main reason for Internet non-use a preference to use their time in other ways.

We had three people who said they ask others to do things for them rather than be users themselves. Only two non-users said they feel disadvantaged in some way by not being able to use the Internet. Other studies have reported that one third of all non-users have asked another person to do something for them on the Internet (Smith, *et al*., 2010, p. 6).

5.2.2 Channel choice

Available literature suggests that channel choice is driven by the perceived value associated with that channel (Broekhuizen & Jager, 2003).

In our study, channel choice was driven by personal preference and type of business activity; trust; previous experience; convenience; control over the information flow in public service provision, particularly the personal information requested by a government agency and the accuracy of personal information; the desire of consistent service; and the desire of holistic need-based service provision.

Research further suggests that online channel adoption is influenced by trust. This is confirmed in our study. For instance, participants often cited security concerns as their reason for not wanting to use online channels. Other participants used online as their default channel and moved to face-to-face only when the online interface lacked sufficient information or customisation for their particular case. Online was preferred for its convenience.

Generally, participants perceived that disclosing private information to a person face-to-face is easier for them and more secure. For instance, all Internet non-users were convinced that face-to-face is preferable and more secure. Also, participants living in minor centres noted the advantage of using face-to-face that they are known to public sector staff. In our study, face-to-face was further preferred by older people, high service dependent people and Pasifika. However, disclosure of personally painful

or distressing private information is preferred to be done over the Internet because of a perception of anonymity.

This study also confirms that people are transferring trust from one e-service environment (e.g. Internet banking, Studylink) to another. These participants were generally aware of the risks associated with working online but appeared to consider these no worse than the risks associated with using other channels.

In accordance with available literature, our research participants often used multiple channels to access public services. Sometimes the participants in our study deployed a single-channel choice strategy towards a particular service, but more often they described using a multi-channel strategy for accessing a public service. For example, participants talked about first finding information online and downloading forms to enable them to see what information they need. This might then be followed up by a phone call and later a face-to-face session. The reasons people gave for their multi-channel strategy are that they want first to find out about the service and what information they need to supply; they then often need to obtain information specific to their individual case, ask questions or seek confirmation. Finally, they provide the requested service-related information via face-to-face or telephone channels, often because they feel this gives them the assurance of receipt.

5.2.3 Trust in government and/or the service providing organisation

Generally, the participants in this study have a high trust in the New Zealand government and its agencies and think that they are working in the best interests of citizens. Exceptions could be found among participants with a high dependency on social services; Māori; Pasifika; and self-employed participants.

In accordance with the literature, participants' trust in a given agency goes hand in hand with their service experience. For instance, one service (Studylink) was fairly consistently linked with a good service and performance experience by participants, leading to increased trust in the organisation and repeated use of the online service.

In terms of the key antecedents to trusting behaviour as described in the international literature, in their perception of government, most participants demonstrated high trust as a result of positive support for benevolence and integrity and negative support for competence and transparency. High service dependents and self-employed participants showed low trust in providing negative support for benevolence, competence (both staff competence and administrative competence or awareness), and transparency; Māori and Pasifika showed low trust and feelings of powerlessness in providing personal information to agencies and citizen identity management by government through negative support for benevolence, integrity and transparency. Furthermore, Māori perceived competence issues related to the use of Māori language by frontline staff.

Furthermore, this study contains evidence that the impact of a negative experience with a public agency can have a strong effect on participants' trust in that particular agency. For instance, poor service performance for some participants, particularly Māori, Pasifika, and high service dependents, was associated with strong feelings of distrust and negative views about how the power-relationship

between the citizen and the service providing agency is played out. Another example is that previous experience had a strong impact on participants' feelings of discomfort with information sharing.

5.2.4 Information sharing

5.2.4.1 Information relationship between the individual and the public sector

Our study shows that participants understand the benefits of identification in a public service relationship, such as the use of the IRD number for authentication in service relationships with IR. However, our participants also noted strong disadvantages of providing the same identification information again later to other public sector staff members of the same organisation. Not only did they perceive this duplication of information provision as a lack of convenience to them, but some of them also wondered what happened to the (bits of) information provided to each staff member. Particularly younger participants had a preference for more convenience through a single process for identity management when dealing with multiple public sector agencies.

Our research participants confirmed the theoretical assumption that what is considered sensitive personal information varies with context and in relationships: participants clearly indicated that the context determines what information needs to be considered private. In the context of public service relationships with New Zealand public service agencies, participants widely considered financial information as sensitive personal information; Māori and Pasifika also perceive details from relatives (e.g. children) as sensitive information.

In their public service relationships with government agencies, privacy preferences of high service dependents, Group 4 participants and Group 5 participants were substantially different from the privacy preferences expressed by other research participants. Whereas most research participants indicated that the sharing of personal information depends on whom they are giving the information to, high service dependents, Group 4 participants and Group 5 participants considered all personal information to be private and therefore only share information with government reluctantly and if they have to.

5.2.4.2 Cross-government information sharing

Theoretical assumptions that cross-agency collaboration and information sharing is not easy and that there are significant barriers to cross-agency information sharing, were not confirmed in the perception of our research participants. Several participants believed that cross-agency information sharing in the New Zealand context is widespread practice. Our research participants generally expressed support for cross-agency information sharing provided that legal conditions, such as the use of information for the lawful purpose and informed consent, are met.

Several research participants however perceived information sharing for monitoring service eligibility and compliance as more contentious: tensions could be observed in perceptions of (potential) personal disadvantages compared to the collective benefits resulting from information sharing.

We did not find any evidence for a lack of confidence among our participants in the corporate governance of public sector organisations responsible for managing citizen identity information.

In our study, young people generally were permissive of cross-agency information sharing. Other participants generally supported information sharing between agencies with close or related mandates and overlapping responsibilities (e.g. Justice, Courts & Police; WINZ & Housing). Reasons for their support were agencies being able to help each other and doing a better job. Some participants also encouraged more and specific cross-agency information sharing, for instance between ACC and IR; between Immigration and IR; between Immigration and Courts; between WINZ and IR; between Courts and IR; and between NZ Police and Transport NZ.

5.2.4.3 Implications of information sharing

In general, our research participants were permissive of cross-agency information sharing but would like to see personal benefit from it. Attributes of both a Service State perspective and a Surveillance State perspective can be observed in the information sharing attitudes of our research participants, with more support among participants for a Service State perspective. For a further discussion about participants' information sharing attitudes with regard to these two perspectives, please see Section 5.3.

Participants generally perceived the following collective benefits from cross-agency information sharing: a fair allocation of taxpayer funded services by stopping people from taking money they are not entitled to and ensuring individuals get the right entitlements; providing the right information to the right agency for the right mandate; avoiding information-loss problems encountered when a client is passed from officer to officer within or across agencies; and the sharing of statistical info for planning purposes (developing new policies and services), providing the right services in the right places, and informing the public.

Participants also observed personal benefits of cross-agency information sharing: convenient and easy to use public services; fairness, as long as you play the game; and efficiency (e.g. taxed at the right rate, no additional tax owing).

However, there was a strong belief among participants that the context determines what personal information can and should be shared, and that the sharing of personal information can have positive and negative outcomes for individuals. In general, participants were uncomfortable about sharing their personal information with agencies they do not know, and agencies with a monitoring function and powers to force compliance.

5.2.5 Informational privacy

In our study, the participant's concept of 'what is private' depended on circumstances. Participants would disclose private information provided they trust the organisation and they see some benefit to them in doing so, such as convenience. This would make our participants what has been called 'privacy pragmatists' in the international literature (6, *et al*., 1998). This privacy pragmatism was evident in all age groups: the younger participants saw it as a trade-off between providing the information and getting the services they want; the high service dependent individuals saw it as what has to be done to obtain the service, but, given a choice, would provide as little information as possible; older participants regarded organisations wanting their private information as 'nosey' and provide it reluctantly.

The younger group particularly felt that what could be considered private is changing in an environment where social networking using Facebook and the like is common, and much once considered 'private' information is readily available via the Internet. This is consistent with the theoretical assumption that new ICTs are changing perceptions of privacy.

Vulnerable individuals (e.g. high service dependent) tended to regard information that could be used against them, or information that might lead to a misjudgement, as private information. High users of social services (including superannuitants) thought they were being asked too much private information and felt they did not have any choice about providing the information asked for because they needed the services to survive.

We do not know from our study whether privacy concerns translate into online behaviour. However, the younger participants did provide insights into their attitudes to online behaviour. They generally make a judgement about the service provider and whether they believe they can be trusted online. They make decisions about what scope and level of private information they are willing to share on the basis of perceived value of the service, their trust in the organisation providing the service, and the degree of privacy threat or intrusion.

Participants had no examples of function creep happening currently or in the future, but they wanted to receive confirmation that information they provide is used for the purpose they gave it (consistent with the rules of the game). The lack of transparency about what information is held about an individual and how that information will be used, was mentioned often by participants.

In our study we did not find any evidence for a tension between privacy and the use of personal information to support public safety.

5.2.6 Trust in the e-service environment: information security

Participants were concerned about the accuracy and security of the information they provide. There was a lack of trust, especially among high service users, that the information they provide is recorded correctly, resulting in incorrect information enduring in the system for a long time without the individual's knowledge. An unexpected positive of digital forms filled in by the applicant was provided when the individual gets to check the information they provide before it is transmitted to the service provider.

Concerns were raised about the competence and integrity of staff recording and using information correctly. Participants felt they are being put in a box but the implications of the information they provide are not transparent to them.

A significant number of participants expressed support for a process that allows them to manage their own personal information. Some online experiences, especially among the younger participants have been positive in terms of building trust in the e-service environment and therefore willingness to provide private information, such as bank account details.

5.2.7 Awareness

There was a general lack of awareness about government agencies, their roles, and the actual extent of current cross-agency information sharing. Younger participants did not distinguish much between

agencies and government as a whole but were generally not comfortable about information sharing by agencies whose role and functions they do not understand. Generally across all the groups, low administrative awareness and lack of knowledge about agencies negatively influenced attitudes to information sharing across agencies.

Furthermore, overall technical awareness of the security risks of operating online were generalised and drew on personal and media anecdotes rather than well informed technical understanding. High users and the younger group also informed this technical understanding with their experiences of using online services, such as online banking. Non-users based much of their technical understanding on media reports.

More than half the groups had some awareness of the Privacy Act and the privacy principles it embodies. Many referred to the restriction it imposes on information being used only for the purpose it was given, unless permission is given to do otherwise. There was also reference to the various administrative procedures government agencies employ to back up the principles of the Act with staff behaviours and practice, although it was sometimes believed that there might be more breeches of these practices than participants feel comfortable with and agencies are aware of. It was widely thought that the current use of privacy disclaimer statements are not actually working as intended: people did not feel they understand what they are agreeing to, why they need to agree to it and what the implications of doing so might be.

5.2.8 Experience, skills, ease of use

Peoples' prior experiences in using government services affected their information sharing attitudes, expectations and future choices about accessing services. In particular, bad or frustrating prior experiences had a stronger negative effect than the positive effect of good experiences on building trust in the service providing organisation. This is consistent with the findings in the international literature that positive experience enhances trust.

Previous experience of e-services influenced individual's administrative and service awareness. An easy-to-use application and/or a good first experience generated a likelihood that the channel would be used again and trust in the agency is increased.

Participants generally found it difficult to find the information relevant to their needs because the information provided is too unsorted or selected and therefore tend to overwhelm.

5.2.9 Transparency

Participants generally found their interactions with government agencies non-transparent in terms of why they need to provide certain information and what it would be used for. People provide the information required with a sense of 'they have to' if they want the service, but there is a lack of reciprocality in the interaction between clients and the government agency. Although it has become common practice for the service user to be asked to agree to information sharing for certain purposes, many felt this is a forced agreement, which they generally do not read because they know they would get no further in the application process unless they agree.

People often did not understand the decision making processes that would be used by the agency or what services might be available.

The information available on government websites is not always easy to find because there is too much information and it is too difficult for people to find the bits that are relevant to them.

A common wish from the participants in our study was that all the information government agencies hold on them as an individual, would be made available to them to check periodically, and amend where necessary. People were worried that government agencies continue to hold old and outdated personal information about them.

A significant number of people in our study would be happy to manage their own personal identity information that is used by government agencies and they would also be happy with a single identity management system provided it is secure and they are able to check and update their own information. They also said they would like to be clearly advised about how their information will be used.

The citizen concerns found in this research are consistent concerns found in the international literature.

5.3 Summary of the meta-analysis

Individuals' acceptance and use of the Internet

1. Scholars generally make a distinction between Internet users, non-users, and ex-users.

This distinction has been used in this research

2. E-Government researchers commonly distinguish between e-Government service use categories of 1) Looking up public sector information online; 2) Interacting with government agencies online; and 3) doing transactions with government agencies online.

This distinction has been used in this research

Channel Choice

3. Channel choice is driven by the perceived value associated with the channel.

In this study, channel choice was driven by personal preference and type of business activity; trust; previous experience; convenience; control over the information flow in public service provision, particularly personal information requested by a government agency and the accuracy of personal information; the desire of consistent service; and the desire of holistic need-based service provision.

4. Online channel adoption is influenced by trust.

This assumption is confirmed in this research

Generally, participants perceived that disclosing private information to a person face-to-face is easier for them and more secure.

This study also confirms that people are transferring trust from one e-service environment (e.g. Internet banking, Studylink) to another.

5. Individuals often use multiple channels to access public services.

This assumption is confirmed in this research

Participants described using a multi-channel strategy for accessing a particular public service: firstly, they find information online and download forms to enable them to see what information they need. This might then be followed up by a phone call and later a face-to-face session.

Trust in government and/or the service providing organisation

6. Citizens' trust in the public service contributes to the broader concept of trust in government. Citizens' trust in government is fluctuating within and across countries, as well as over time.

*Generally, the participants in this study have a high trust in the New Zealand government and its agencies and think that they are working in the best interests of citizens. Exceptions could be found among participants with a high dependency on social serv**ices; Māori; Pasifika; and self**-employed.*

7. The key antecedents to trusting behaviour are competence, benevolence, integrity, and transparency.

In their perception of government, most participants demonstrated high trust as a result of positive support for benevolence and integrity, and negative support for competence and transparency; high service dependents and self-employed participants showed low trust in providing negative support for benevolence,

competence (both staff competence and administrative ***competence or awareness), and transparency; Māori*** *and Pasifika showed low trust and feelings of powerlessness in providing personal information to agencies and citizen identity management by government through negative support for benevolence, integrity and* ***transparency. Furthermore, Māori perceived competence issues related to the use of Māori language by*** *frontline staff.*

8. An individual's trust in government is related to their own experience of government and public service consumption, personal experiences of family members and friends, and through stories in the media.

In this research, this assumption is only confirmed for having a negative experience with a government agency: this had a strong effect on participants' trust in that particular agency. Some participants, particularly ***Māori, Pasifika, and high service dependents, associated poor service performance with strong feelings of*** *distrust and negative views about how the power-relationship between the citizen and the service providing agency is played out.*

9. To public service customers, the impact of a negative experience with a public agency is much more pronounced than the effect of a positive experience.

This assumption is confirmed in this research

Information Sharing

10. An individual can use a variety of personal 'identifiers' to present herself in a public service relationship.

This assumption is confirmed in this research. This study shows that participants understand the benefits of identification in a public service relationship (e.g. using the IRD number). However, our participants also noted strong disadvantages of providing the same identification information again later to other public sector staff members. Not only did they perceive this duplication of information provision as a lack of convenience to them, but some of them also wondered what happened to the information provided to each staff member involved.

Particularly younger participants had a preference for more convenience through a single process for identity management when dealing with multiple public sector agencies.

11. What is considered sensitive personal information varies with context and in relationships

This assumption is strongly confirmed in this research: participants clearly indicated that the context determines what information needs to be considered private. In the context of public service relationships with New Zealand public service agencies, participants widely considered financial information as sensitive ***personal information; Māori and Pasifika also perceive*** *details from relatives (e.g. children) as sensitive information.*

12. Individuals' privacy preferences exhibit finely tuned tendencies to disclose, share, and withhold personal information, depending on context, relationship, and type of information.

This assumption is confirmed in this research

In this study, the privacy preferences of high service dependents, self-employed participants and super-annuitants were substantially different from the privacy preferences of other research participants. Whereas most research participants indicated that the sharing of personal information depends on whom they are giving the information to, high service dependents, self-employed and super-annuitants considered all personal information to be private and therefore only shared information with government reluctantly and if they had to.

Cross-agency information sharing

13. Cross-agency collaboration is not easy, and takes time and additional effort by individuals and agencies involved. The more the clients' needs are interrelated and need to be addressed by multiple agencies, the more government agencies need to collaborate to address their information deficiencies.

This assumption is not confirmed in the perception of the participants in this research. Several participants believed that cross-agency information sharing in the New Zealand context is widespread practice.

14. International research findings demonstrate that there are many cases where a citizen's personal information is still not shared when it should be, or where it is shared when it should not be.

This assumption is partly confirmed in this research.

Participants generally expressed support for (more) cross-agency information sharing provided that legal conditions, such as the use of information for the lawful purpose and informed consent, are met.

Participants generally supported information sharing between agencies with close or related mandates and overlapping responsibilities (e.g. Justice, Courts & Police; WINZ & Housing). Reasons for their support were agencies being able to help each other and doing a better job. Some participants also encouraged more and specific cross-agency information sharing, for instance between ACC and IR; between Immigration and IR; between Immigration and Courts; between WINZ and IR; between Courts and IR; and between NZ Police and Transport NZ.

Several research participants however perceived information sharing for monitoring service eligibility and compliance as more contentious: tensions could be observed in perceptions of (potential) personal disadvantages compared to the collective benefits resulting from information sharing.

15. Research shows significant barriers to cross-agency information sharing in organisational, political and legal, and technical domains.

This assumption is not confirmed in the perception of the participants in this research

16. International research suggests a lack of confidence in corporate governance of organisations responsible for collecting, storing and sharing significant amounts of personal information.

This assumption is not confirmed in this research

Implications of information sharing

17. Available literature points at two different perspectives on the management of citizen identity information in e-government service environments: a 'Surveillance State' perspective and a 'Service State' perspective (see Figure 4). UK-based research suggests that attributes of both perspectives can be observed in e-government service environments when looking at the actual use of citizen identity information.

This assumption is confirmed in this research

In general, participants are permissive of cross-agency information sharing but would like to see personal benefit from it. Attributes of both a Service State perspective and a Surveillance State perspective can be observed in the information sharing attitudes of the research participants, with more support for a Service State perspective.

However, there was a strong belief among participants that the context determines what personal information can and should be shared, and that the sharing of personal information can have positive and negative outcomes for individuals. In general, participants were uncomfortable about sharing their personal information with agencies they don't know, and agencies with a monitoring function and powers to force compliance.

Information privacy

18. Privacy is a multifaceted, ambiguous notion which means many things to many people.

This assumption is confirmed in this research

In this study, the participant's concept of 'what is private' depended on circumstances. Participants would disclose private information provided they trust the organisation and they see some benefit to them in doing so, such as convenience. This would make our participants what has been called 'privacy pragmatists' in the international literature (6, et al., 1998).

Vulnerable individuals (e.g. high service dependent) tended to regard information that could be used against them, or information that might lead to a misjudgement, as private information. High users of social services thought they were being asked too much private information and felt they did not have any choice about providing the information asked for because they needed the services to survive.

19. The meaning of informational privacy is changing under the possibilities opened up by new ICTs.

This assumption is confirmed in this research

Particularly younger participants felt that what could be considered private is changing in an environment where social networking is common and much once considered 'private' information is readily available via the Internet.

20. Concerns expressed about privacy do not necessarily translate to online behaviour.

This assumption has not been explored in this research

21. There is a tension between privacy and the use of personal information to achieve more convenient public services for citizens.

This assumption is confirmed in this research. Participants perceive providing personal information as a trade-off for getting the services they want and/or are entitled to. High service dependent participants perceive providing their personal information as something what has to be done to obtain the service they need.

22. There is a tension between privacy and the use of personal information to support public safety.

We did not find any evidence for this tension in this study

23. Available literature points at possibilities of 'function creep' or 'mission creep'.

This assumption is not confirmed in the perception of participants in this research; however, participants wanted to receive confirmation that information they provide is used for the purpose they gave it for, consistent with the 'rules of the game'. The lack of transparency about what information is held about an individual and how that information will be used was mentioned often by participants.

Trust in the e-service environment: information security

24. Robust identity management is identified as an enabler of trust in e-government service environments.

This assumption is confirmed in this research

25. Dominant barriers to online public service consumption relate to an individual's perception of risks associated with the online environment.

This assumption is confirmed in this research

26. Threats to the security of personal information can come from human fallibility, technological fallibility, or from the interaction between human and technological fallibility.

This assumption of human fallibility is strongly confirmed in this research

There was a lack of trust among participants that the information they provide is recorded correctly, resulting in incorrect information enduring in the system for a long time without the individual's knowledge. An unexpected positive of digital forms filled in by the applicant was provided when the individual gets to check the information they provide before it is transmitted to the service provider.

Concerns were raised about the competence and integrity of staff recording and using information correctly. Participants felt they are being put in a box but the implications of the information they provide are not transparent to them.

A significant number of participants expressed support for a process that allows them to manage their own personal information.

Awareness

27. People have little awareness of what personal information is held by public sector agencies.

This assumption is strongly confirmed in this research. Generally, across all the groups, low administrative awareness and lack of knowledge about agencies negatively influenced attitudes to information sharing across agencies.

28. People operating in online environments lack crucial knowledge about privacy practices and available tools.

This assumption is not confirmed in this research.

More than half the groups had some awareness of the Privacy Act and the privacy principles it embodies. Many referred to the restriction it imposes on information being used only for the purpose it was given, unless permission is given to do otherwise.

It was widely thought that the current use of privacy disclaimer statements are not actually working as intended: people did not feel they understand what they are agreeing to, why they need to agree to it and what the implications of doing so might be.

Experience, skills, ease of use

29. Previous experience, training and skills, and Internet access, support the uptake of e-government services. A barrier to e-government service uptake is familiarity and comfort with existing service channels.

Peoples' prior experiences in using government services affected their information sharing attitudes, expectations and future choices about accessing services.

Previous experience of e-services influenced individual's administrative and service awareness. An easy-to-use application and/or a good first experience generated a likelihood that the channel would be used again and trust in the agency is increased.

Participants generally found it difficult to find the information relevant to their needs because the information provided is too unsorted or selected and therefore tend to overwhelm.

Transparency

30. There is a lack of transparency around ICT-enabled information aggregation and analysis in varying relationships between individuals and organisations.

A modified version of this assumption is strongly confirmed in this research: generally, there is a lack of transparency around information sharing in varying service relationships between individuals and government agencies.

Participants generally found their interactions with government agencies non-transparent in terms of why they need to provide certain information and what it would be used for. People provide the information required with a sense of 'they have to' if they want the service, but there is a lack of reciprocality in the interaction between clients and the government agency.

People often did not understand the decision making processes that would be used by the agency or what services might be available.

The information available on government websites is not always easy to find because there is too much information and it is too difficult for people to find the bits that are relevant to them.

31. Transparency enhances the protection and security of citizen identity information by supporting citizens' control over their personal information.

This assumption is strongly confirmed in this research

A common wish from the participants in our study was that all the information government agencies hold on them as an individual, would be made available to them to check periodically, and amend where necessary. People were worried that government agencies continue to hold old and outdated personal information about them.

A significant number of people in our study would be happy to manage their own personal identity information that is used by government agencies and they would also be happy with a single identity management system provided it is secure and they are able to check and update their own information. They also said they would like to be clearly advised about how their information will be used.

6. Implications of the Research Findings

6.1 Surveillance State vs. Service State perspectives

Our research findings demonstrate that the majority of participants had a benign view of information sharing intentions and practice in the New Zealand public sector. Most of them displayed at least two of the key antecedents to trusting behaviour towards the New Zealand public sector, namely benevolence and integrity.

With a few exceptions, our research population turned out to be privacy pragmatists: individuals who are prepared to provide personal information to organisations in return for enhancements of public service provision or other personal or collective benefits. Some of our participants even advised on opportunities for more cross-agency information sharing so that personal and collective benefits of public service provision could be further enhanced.

Our research participants were not unconcerned about their privacy and clearly pointed at information security risks and the need for public service agencies to play privacy by the rules by using provided information only for the intended purpose and asking clients for consent. Consequently, there does not seem to be a perception of eroding trust or the violation of privacy rights. Therefore, a Service State perspective seems to be predominant among most of our research participants.

However, we also observe that one of the key antecedents of trusting behaviour, transparency, was generally absent amongst our participants. For instance, participants generally were uncomfortable about sharing information with agencies they did not know. Moreover, as a result of low administrative awareness, participants did not have the 'competence' of understanding (the variety of) public sector organisations and public service relationships. Participants indicated they provide their information to public sector agencies because they need to do so in order to get the service, but they usually do not understand how their information will be processed or used, why they need to fill in multiple forms with the same information, how and to what length their information will be stored or kept, and who will have access to their information, for instance.

Furthermore, participants showed limited knowledge about the sharing - or non-sharing - of information between agencies. These deficiencies of transparency and administrative competence led participants to be uncomfortable about information sharing and wanting to have more control over personal information provided to public sector agencies. This particular response was stronger among those participants who were more distrustful of government agencies, such as the self-employed, Pasifika, Māori, and beneficiary groups.

An area of concern to a number of research participants was the accuracy of personal information stored and processed by government agencies, and particularly information used for categorising clients and determining eligibility for services. Some research participants, particularly those with high service dependency, self-employed South-Islanders, Pasifika, and Māori, demonstrated a Surveillance State perspective towards the processing of personal information into the system, such as perceptions of staff using the power of their position, ethnicity as a target for (more) public services, and 'social

sorting' activities by case managers deliberately 'putting you in the box' and 'you don't have a say about something we think might be unrealistic'.

Several research participants from other groups noted a problem with incompetent front-line staff members making mistakes with the handling and processing of personal information (e.g. typos, mis-spelling, and mispronunciation) or providing a different answer to the same query put forward to another staff member of that particular public service organisation. If this problem of staff incompetency did not seem to substantially influence participants' trust behaviour towards public sector agencies, it did have an effect on some participants' preference for more control over their personal information.

Participants not only expressed negative concerns around information accuracy, there was also the concern that frontline staff members were not asking for the relevant information to provide the right service. Put differently, several participants had the view that public sector agencies do not provide holistic needs-based services in accordance with the Service State perspective, but tend to stick to standardised form-filling in accordance with the agency's information requirements. Furthermore, participants expressed difficulties in finding and joining up the bits of public service information that are relevant to them.

Research participants particularly experienced these limitations of standardised form-filling and the lack of relevant and integrated public service information in accessing public services online. For some, the lack of provision for adding relevant information to their individual case on an online form was the reason they prefer to speak to a staff member rather than using the e-channel for public service consumption. However, limited integration of public service information and public services was also experienced in the real world, where participants needed to deal with various staff members within or across public sector agencies in order to meet their particular service need.

A tension in participants' perspectives could be observed in discussing the advantages and disadvantages of cross-agency information sharing at a collective level of interest and at a personal level of interest. The majority of participants saw clear benefits of cross-agency information sharing at a collective level of interest, such as increased effectiveness in public service provision to individuals, fair allocation of taxpayer funded services and improved service quality, and therefore were permissive. Several participants also pointed at advantages of cross-agency information sharing at a personal level, such as simple and convenient public services, fair public service provision for those who play the game in accordance with the rules, efficient public service provision (e.g. avoiding untimely discovery of overpayments), and improved quality of public service provision.

However, if participants perceived (potential) disadvantages of cross-agency information sharing at a personal level of interest, they tended to be more protective of their personal information and pointed at the requirement of privacy protection. For instance, vulnerable individuals, particularly those highly dependent on social services, tended to regard information that could be used against them, or information that might lead to a misjudgement in public service provision, as private information. A few participants, for instance in the non-user group, pointed at the possibility of false accusations, which was a reason for them to be uncomfortable in sharing information with the Police, CYF or WINZ. Other high users of social services, such as the superannuitants, thought they were being asked too much private information and felt they did not have any choice about providing the requested information as they needed the service. Furthermore, participants generally felt uncomfortable in sharing personal

information with agencies with an eligibility monitoring function and powers to force compliance. A useful summary of this tension was provided in Group 1, where participants pointed out:

> What information can and should be shared depends on the information . . . there is a lot of personal stuff that can make or break peoples' lives.

6.2 An emerging scenario in the New Zealand context: a Fair State perspective

We observed that most of our research participants perceive attributes belonging to a Service State perspective in their attitudes towards information sharing, such as better public service provision and increased service effectiveness; only some of them demonstrated attributes of a Surveillance State perspective, such as increased information asymmetries, eroded trust, social sorting and putting people in the wrong box.

We also observed that, although research participants generally support cross-agency information sharing for the achievement of a Service State perspective, they don't see quite a few attributes of a Service State perspective, such as reduced duplication, holistic needs-based service provision and improved access to public services, in the public service relationships they have experienced thus far. Instead, research participants referred to attributes which neither belong to a Service State perspective nor a Surveillance State perspective. These attributes appear to constitute an alternative scenario among our research participants, a Fair State perspective. The following attributes can be observed under this alternative perspective:

Table 12: Fair State perspective

Attribute	Fair State Perspective Meaning
Increased and systematic use of digital citizen IDM systems	Efficiency support systems leading to value for the taxpayer's money and treating citizens fairly
IDM objective	Increased processing and rationing of public service clients; increased efficiency and equitable enforcement
Purposeful attention to citizen identity information	Fairness in public service use
Increased information sharing	Improved decision-making by individual public service providing agencies; Improved compliance; Increased efficiency for citizens in their role as taxpayer and public service customer
Client focus	Improved administration; fair and equitable public service provision; organisation-centric government
Implications for citizen-government relationships	Information asymmetries in citizen-government relationships are clear and applicable to all;
Citizen rights' implications	Equality under the Law

The three perspectives of the Surveillance State, the Service State and the Fair State compare as follows (adapted from Lips *et al*, 2009):

Table 13: The Surveillance State, the Service State and the Fair State

Attribute	Surveillance State Perspective Meaning	Service State Perspective Meaning	Fair State Perspective Meaning
Increased and systematic use of digital citizen IDM systems	Surveillance systems leading to rationalization and control	Public service support systems leading to service transformation	Efficiency support systems leading to value for the taxpayer's money and treating citizens fairly
IDM objective	Risk management, 'knowing the unknown'; increased efficiency	Targeted public service provision; CRM; increased effectiveness	Increased processing and rationing of public service clients; increased efficiency and equitable enforcement
Purposeful attention to citizen identity information	Surveillance	Better public service provision	Fairness in public service use
Increased information sharing	Increased analysis; matching and merging of citizen identity information; profiling	Reduced duplication and fragmentation; joined-up government; integrated public service provision	Improved decision-making by individual public service providing agencies; Improved compliance; Increased efficiency for citizens in their role as taxpayer and public service customer
Client focus	Monitoring; segmentation of service users; social sorting	Holistic needs-based service provision; personalization; citizen-centric government	Improved administration; fair and equitable public service provision; organisation-centric government
Implications for citizen-government relationships	Increasing information asymmetries; eroding trust	Decreasing information asymmetries; increasing trust	Information asymmetries in citizen-government relationships are clear and applicable to all;
Citizen rights' implications	Violation of privacy and individual freedom rights	Improved access to public services; open government, transparency	Equality under the Law

6.3 Contextual integrity

Our research findings strongly support the theoretical viewpoint that context determines peoples' attitudes towards information sharing in public service environments and privacy implications. The following context-related factors appeared to be of particular importance to our research participants in their attitudes towards information sharing in the course of public service provision.

Firstly, we observed substantial differences between the majority of our research population and specific groups within that population. We noted differences in information sharing attitudes of those participants with high service dependence; participants who are self-employed and living in a major South Island community; Māori participants; and Pasifika participants. For instance, whereas most participants did not see a problem with sharing their personal information with government as long as privacy principles like information use for purpose and informed consent are applied, high service dependent participants and those who are self-employed perceived all personal information as private information and only wanted to share information with government reluctantly and if they have to, as government is 'not working for them'. High service dependent participants saw clear negative power imbalances and information asymmetries between themselves and public sector agencies. These negative feelings of distrust and powerlessness towards public sector agencies were also present among Māori and Pasifika participants with some subtle differences between these two groups: for instance, whereas Māori particularly were negative about the integrity and Māori language use of

individual public service staff members, Pasifika people found dealing with government agencies difficult and felt demeaned by the process.

Secondly, participants generally supported information sharing between agencies with close or related mandates and overlapping responsibilities. Roughly, we observed that participants make a distinction between the following service clusters: a financial service cluster (e.g. IR & ACC), a social service cluster (e.g. WINZ & Housing), a justice service cluster (e.g. Police, Courts, Immigration & Justice) and a health service cluster[3]. Underlying reasons for participants to be supportive of cross-government information sharing within these service clusters are that agencies can help each other and do a better job. In terms of trust, participants more or less had the same attitude towards agencies within a service cluster; however, previous experience with a specific agency could lead to different trust behaviour towards that particular agency compared to other agencies in the same service cluster.

Thirdly, participants did not treat public service channels as separate contexts for information sharing, but perceived the public service context for information sharing at the level of their particular service need. This could imply for instance that participants used a multi-channel strategy in order to get the best service to meet their need, or that they tried to speak to various staff members within or across government agencies. Another example is that participants usually did not understand why they needed to fill in multiple forms with similar information to meet their particular service need. We can conclude from this that there can be a tension between participants' 'horizontal' attitudes towards information sharing for the purpose of meeting their service need and the 'vertical' organisation and focus of public sector agencies in public service provision.

Finally, due to the fact that participants often perceived a lack of transparency around information sharing with and between public sector agencies, they also did not have a clear context in which they share personal information with public sector agencies. This situation increased discomfort amongst participants, including feelings of information asymmetries and a lack of control over personal information. Consequently, participants' attitudes towards information sharing and privacy implications were coloured as a result of unclear contextual boundaries for information sharing practice and lacking knowledge on the integrity of personal information shared with public sector agencies.

Based on these research findings, we suggest that a contextual approach within each of these four areas should be taken in the design and development of information sharing in the course of e-government service provision. If public sector agencies would like to actually achieve a Service State Perspective in the citizens they interact with, our research suggests a different approach of contextual integrity of information sharing needs to be developed and managed for the following clusters and sectors:

- Information sharing integrity and transparency within clear contextual boundaries for information sharing practice;
- Information sharing integrity within the context of a specific customer target group, such beneficiaries, Māori, Pasifika, or self-employed;
- Information sharing integrity within the context of a specific service cluster, such as a financial service cluster, social service cluster, justice service cluster or health service cluster;
- Information sharing integrity within the context of a multi-channel-strategy; and

[3] Research participants were informed that health information is outside the scope of this research.

- Information sharing integrity within the context of a customer's service need.

6.4 Recommendations for further research

As discussed earlier, this research activity involved a research population of 63 members of the New Zealand general public, which sets limitations to the generalisation of the research findings. Furthermore, we only explored peoples' attitudes towards information sharing in the course of online public service provision and therefore did not investigate peoples' actual online behaviour. On the basis of these research design limitations we would like to make the following recommendations for further research:

- Further research into information sharing and privacy attitudes from individuals belonging to the four distinct clusters identified in this research: high service dependents; self-employed; Māori; and Pasifika;
- Further research into information sharing and privacy attitudes from Internet ex-users;
- Further research into peoples' attitudes and behaviour towards using multi-channel strategies for meeting a service need.
- An ethnographic study of the actual online behaviour of New Zealanders using e-government services;
- An exploration of potential transparency models and an evaluation of their effectiveness in a New Zealand e-government service context; and
- A qualitative study of peoples' attitudes and behaviour towards integrated e-government service environments with implemented forms of increased transparency and/or control over personal information.

References

6, P. (1998). *The future of privacy* (Vol. 1: Private life and public policy). London: Demos.

6, P. (2004). Joined-up government in the western world in comparative perspective: A preliminary literature review and exploration. *Journal of Public Administration Research and Theory, 14*(1), 103–138.

6, P., Lasky, K., & Fletcher, A. (1998). *The future of privacy* (Vol. 2: Public Trust and the use of private information). London: Demos.

6, P., Raab, C., & Bellamy, C. (2005). Joined-up government and privacy in the United Kingdom: Managing tensions between data protection and social policy. Part 1. *Public Administration, 83*(1), 111-133.

Andersen, K. V., & Henriksen, H. Z. (2006). E-Government maturity models. Extension of the Layne & Lee model. *Government Information Quarterly, 23*, 236-248.

Australian Communications and Media Authority (2009). Attitudes Towards Use of Personal Information Online: Qualitative Research Report: ACMA.

Australisan Communications and Media Authority (ACMA) (2009). *Attitudes Towards Use of Personal Information Online: Qualitative Research Report*.

Backhouse, J., & Halperin, R. (2006). *A survey on EU citizen's trust in ID systems and authorities.* London School of Economics and Political Science, Department of Management Information Systems and Innovation Group, London.

Backhouse, J., & Halperin, R. (2007). A Survey on EU Citizen's Trust in ID systems and authorities. *FIDIS Journal, 1/2007*.

Bannister, F. (2007). *Trust and Transformative Government*. Paper presented at the 2007 EGPA Conference, 19-22 September 2009.

Barnes, C., & Gill, D. (2000). *Declining Government Performance? Why Citizens Don't Trust Government*. Wellington: State Services Commission.

Bellamy, C., 6, P., Raab, C., Warren, A., & Heeney, C. (2008). Information sharing and confidentiality in social policy: Regulating multi-agency working. *Public Administration, 86*(3), 737–759.

Bellamy, C., 6, P., & Raab, C. D. (2005). Joined-up Government & Privacy in the United Kingdom: Managing Tensions between Data Protection and Socialy Policy, Part 2. *Public Administration, 83*(2), 393-415.

Bellamy, C., Raab, C., Warren, A., & Heeney, C. (2007). Institutional shaping of interagency working: Managing tensions between collaborative working and client confidentiality. *Journal of Public Administration Research and Theory, 17*(3), 405–435.

Bellamy, C., & Taylor, J. A. (1998). *Governing in the Information Age*. Buckingham: Open University Press.

Bennett, C. J., & Raab, C. (2003). *The governance of privacy: Policy instruments in global perspective*. Aldershot, UK: Ashgate.

Bertot, J. C., & Jaeger, P. T. (2008). The E-Government paradox: Better customer service doesn't necessarily cost less. *Government Information Quarterly, 25*(2), 149-154.

Birch, D. G. W. (2007). *Digital Identity Management. Perspectives on the technological, business and social implications*. Aldershot: Gower Publishing Limited.

Bok, D. (2001). *The Trouble with Government*. Cambridge: MA: Harvard University Press.

Broekhuizen, T. L. J., & Jager, W. (2003). *A conceptual model of channel choice: Measuring online and offline shopping value perceptions*. The Netherlands: University of Groningen.

Bryson, J. M., Crosby, B. C., & Middleton Stone, M. (2006). The design and implementation of cross-sector collaborations: Propositions from the literature. *Public Administration Review*(Special Issue), 44–55.

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U.-D. (2007). Development of measures of online privacy concern and protection for use on the onternet. *Journal of the American Society for Information Science and Technology, 58*(2), 157-165.

Burgoon, J. K., Parrott, R., LePoire, B. A., Kelly, D. L., Walther, J. B., & Perry, D. (1989). Maintaining and restoring privacy through communication in different types of relationship. *Journal of Social and Personal Relationships, 6*, 131-158.

Camp, J. (2003). Identity in Digital Government: A Research Report of the Digital Government Civic Scenario Workshop. Retrieved from http://www.ljean.com/files/identity/pdf

Castells, M. (2009). *Communication Power*. Oxford, UK: Oxford University Press.

Clarke, R. (1988). Information Technology and Dataveillance. *Communications of the AMC, 37*(5), 498-512.

Clarke, R. (1994). Human Identification in Information Systems: Management Challenges and Public Policy Issues. *Information Technology & People, 7*(4), 6-37.

Conklin, E. J. (2006). *Dialogue mapping. Building shared understanding of wicked problems*. England: John Wiley and Sons.

Connolly, R., & Bannister, F. (2007). Consumer trust in Internet shopping in Ireland: towards the development of a more effective trust measurement instrument. *Journal of Information Technology, 22*, 102-118.

Crompton, M. (2008). *User Centric Identity Management: An oxymoron or the key to getting identity management right?* Paper presented at the Managing Identity in New Zealand: Identity Conference 2008.

Crossman, G. (2007). The ID Problem. In D. G. W. Birch (Ed.), *Digital Identity Management. Perspectives on the Technological, Business and Social Implications* (pp. 175-182). Aldershot: Gower Publishing Limited.

Das, T. K., & Teng, B. (2001). Trust, control and risk in strategic alliances: An integrated framework. *Organization Studies, 22*(2), 251-283.

DeCew, J. W. (1997). *In pursuit of privacy: Law, ethics and the rise of technology*. Ithaca, NY: Cornell University Press.

Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. (2006). *Digital Era Governance: IT Coporations, the State, and E-Government*. Oxford: Oxford University Press.

Dutton, W. H., Helsper, E. J., & Gerber, M. M. (2009). Oxford Internet Survey 2009 Report: The Internet in Britain. Oxford, UK: Oxford Internet Institute, University of Oxford.

Dyer, J. H., & Chu, W. (2003). The role of trustworthiness in reducing transaction costs and improving performance: Empirical evidence from the United States, Japan and Korea. *Organization Science, 14*(1), 57-68.

Edelenbos, J., & Klijn, E.-H. (2007). Trust in complex decision making networks: A theoretical and empirical exploration. *Administration and Society, 39*(1), 25-50.

Eppel, E., Gill, D., Lips, A. M. B., & Ryan, B. (2008). *Better connected services for Kiwis: A discussion document for managers and front line staff on better joining up the horizontal and the vertical*. Wellington: Institute of Policy Studies, School of Government, Victoria University of Wellington.

Eurostat Information Society Statistics 2009. European Commission, from http://epp.eurostat.ec.europa.eu/portal/page/portal/information_society/data/database

FIDIS (2006). Future of Identity in the Information Society: Identity in a Networked World - Use Cases and Scenarios. Retrieved from http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp2-del2.6_Idendity_in_a_Networked_World.pdf

Filipe Araujo, J. (2001). Improving Public Service Delivery: The Crossroads between NPM and Traditonall Bureaucracy *Public Administration* (Vol. 79, pp. 915-932). Oxford: Balckwell Publishers Ltd.

Fox, S. (2000). Trust and Privacy Online: Why Americans Want to Rewrite the Rules. Retrieved from www.pewinternet.ort/Reports/2000/Trust-and-Privacy-Online.aspx

Gandy, O. (1993). The Panoptic Sort: A Political Economy of Personal Information. Boulder: Westview Press.
Gavison, R. (1980). Privacy and the Limits of the Law. *Yale Law Journal, 89*, 421-471.
Gellman, R. (2004). Privacy and security: Assessing database derivative activities. *Government Information Quarterly, 21*, 498-504.
Gil-Garcia, J. R., Chengalur-Smith, I., & Duchessi, P. (2007). Collaborative e-government: Impediments and benefits of information sharing projects in the public sector. *European Journal of Information Systems, 16*, 121-133.
Greenwood, D. (2007). *The Context for Identity Management Architectures and Trust Models*. Paper presented at the OECD Workshop on Digital Identity Management.
Halperin, R., & Backhouse, J. (2008). A roadmap for research on identity in the information society. *Identity in the Information Society, 1*,
Heintzman, R., & Marson, B. (2005). People, service and trust: Is there a public sector service value chain. *International Review of Administrative Sciences, 71*(4), 549-575.
Her Majesty's Revenue and Customs (2008). *The customer experience of online filing: Final Inland Revenue (2008). Annual Report 2008-2011*. Wellington: Inland Revenue.
Hood, C. (1991). A Public Management for all Seasons? *Public Administration, 69*(Spring 1991), 3-19.
House of Lords Select Committee on the Constitution (2009). Surveillance: Citizens and the State (Vol. I:Report). London: The Stationery Office Ltd.
Institute for Citizen-Centred Service (2008). Citizens First 5. Canada: Institute for Citizen-centred Service.
Institute for Insight in the Public Services (2008). Data and Privacy: How Concerned are Citizens about Data Sharing in the Public Service? London: Institute for Insight in the Public Services.
Kampen, J. K., van de Walle, S., & Bouckaert, G. (2006). Assessing the Relation between Satisfaction with Public Service Delivery and Trust in Government. The impact of the predisposition of Citizens Toward Government on Evaluations of Its Performance. *Public Performance & Management Review, 29*(4), 387-404.
Kelly, G., & Hopkins-Burns, V. (2010). *Building Bridges to the Community: Using Customer-Centric Measures of Satisfaction and Perceptions*. Paper presented at the 9th International Tax Administration Conference (ATAX).
Klijn, E.-H. (1997). Policy networks: An overview. In W. J. Kickert, E.-H. Klijn & J. F. M. Koppenjan (Eds.), *Managaing complex networks: Strategies for the public sector* (pp. 14–34). London, Thousand Oaks, New Delhi: Sage Publications.
Koops, B.-J., Buitelaar, H., & Lips, A. M. (2007). D5.4: Anonymity in Electronic Government: A Case-Study Analysis of Governments' Identity Knowledge. *Future of Identity in the Information Society (FIDIS)*.
KPMG (2008). *Data Loss Barometer*: KPMG, LLP, UK.
Krasnova, H., Gunther, O., Spiekermann, S., & Koroleva, K. (2009). Privacy concerns and identity in online social networks. *Identity and the Information Society, 2*, 39-63.
Layne, K., & Lee, J. (2001). Developing fully functional E-government: A four stage model. *Government Information Quarterly, 18*(2).
Lee, M., & Turban, E. (2001). A Trust Model for Consumer Internet Shopping. *International Journal of Electronic Commerce, 6*(1), 75-91.
Lips, A. M. B. (2008). Identity Management in Informaiton Age Government. Exploring concepts, definitions, approaches and solutions. *Working paper, June 2008*, 56. Retrieved from http://www.e.govt.nz/services/authentication/library/docs/idm-govt-08.pdf
Lips, A. M. B., O'Neill, R., & Eppel, E. (2009c). Improving Information Sharing for Effective Social Outcomes. Wellington: Victoria University of Wellington.
Lips, A. M. B., Taylor, J., & Organ, J. (2006). Identity Management as Public Innovation: Looking Beyond ID Cards and Authentication Systems. In V. J. J. M. Bekkers, H. P. M. van

Duivenboden & M. Thaens (Eds.), *ICT and Public Innovation: assessing the modernisation of public administration*. Amsterdam: IOS Press.
Lips, A. M. B., Taylor, J. A., & Organ, J. (2009a). Identity management, administrative aorting and citizenship in new modes of government. *Information, Communication and Society, 12*(5), 715-734.
Lips, A. M. B., Taylor, J. A., & Organ, J. (2009b). Managing citizen identity information in e-government service relationships in the UK: The ememrgence of a surveillance state or a service state? *Public Management Review, 11*(6), 833-856.
Livingstone, S., & Bober, M. (2004). UK Children Go Online: Surveying the experiences of young people and their parents. UK: London School of Economics and Political Science.
London School of Economics (2005). The Identity Project. An assessment of the UK Identity Cards Bill and its implications: The LSE Identity Project Final Report, June 2005.
Lusoli, W., Maghiros, I., & Bacigalupo, M. (2009). eID policy in a turbulent environment: Is there a need for a new regulatory framework? *Identity in the Information Society*.
Lusoli, W., & Miltgen, C. (2009). Young people and emerging digital services: An exploratory survey on motivations, perceptions and acceptance of risks. In W. Lusoli, R. Campano & I. Maghiros (Eds.), *JRC Scientific and Technical Reports*. Accessed 23 July, 2020 at http://ftp.jrc.es/EURdoc/JRC50089.pdf: JRC, European Commission.
Lyon, D. (2001). *Surveillance Society. Monitoring everyday life*. Buckingham: Open University Press.
Lyon, D. (2003). Surveillance as social sorting. Computer codes and mobile bodies. In D. Lyon (Ed.), *Surveillance & Social Sorting: privacy, risk and digital discrimination* (pp. 13-30). London: Routledge.
Lyon, D. (2006). *Theorizing Surveillance. The panopticon and beyond*. Cullompton: Willan publishing.
Lyon, D. (2007). Surveillance Studies: An Overview. Cambridge: Polity Press.
Madden, M., & Smith, A. (2010). Reputation Management and Social Media: How people monitor their identity and search for others online. Washington, DC: Pew Internet &American Life Project, Pew Research Center.
Malhotra, N., Sung, S. K., & James, A. (2004). Internet Users' Information Privacy Concerns (IUIPC): The construct, the scale, and a casual model. *Information Systems Research, 15*(4), 366-355.
Margetts, H. (2003). Electronic Government: A Revolution in Public Administration? In B. G. Peters & J. Pierre (Eds.), *Handbook of Public Administration* (pp. 366-376): Sage.
Marx, G. T. (2004). What's New About the "New Surveillance"? Classifying for Change and Continuity. *Knowledge, Technology, and Policy, 17*(1), 18-37.
Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *Academy of Management Review, 20*(3), 709-734.
Millard, J. (2006). User Attitudes to E-Government Citizen Services in Europe. *International Journal of Electronic Government Research, 2*(2), 49-58.
Moore, B. (1984). *Privacy: Studies in social and cultural history*. Amonk, NY: M.E Sharpe.
MORI (2003). Privacy and Data Sharing for Department for Constitutional Affairs: Survey of Public Awareness and Perceptions. London: Department of Constitutional Affairs.
Mossberger, K., Tolbert, C. J., & McNeal, R. S. (2008). *Digital Citizenship. The Internet, society, and participation*. Cambridge MA & London: The MIT Press.
Murakami-Wood, D., Ball, K., Lyon, D., Norris, C., & Raab, C. D. (2006). A Report on the Surveillance Society: September 2006, for the Information Commissioner by the Surveillance Studies Network, Full Report available at: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf.
Muthusamy, S. K., & White, M. K. (2005). Learning and knowledge transfer in strategic alliances: A social exchange view. *Organization Studies, 26*(3), 415-441.

National Research Unit (2009). Measuring Customer Satisfaction with Online Services: Developing a Model of Satisfaction with Online Services. New Zealand: Inland Revenue.
Nissenbaum, H. (2010). *Privacy In Context: Technology, Policy and the Integrity of Social Life*. California: Stanford University Press.
Norris, P. (2001). *Digital Divide: civic engagement, information poverty, and the Internet worldwide*. Cambridge: Cambridge University Press.
O'Harrow, R. (2005). *No Place to Hide*.
OECD Directorate for Science Technology and Industry (2001). Understanding the Digital Divide. Paris: OECD.
OECD Directorate for Science Technology and Industry (2008). *At the crossroads: "Personhood" and digital identity in the information society. Working paper 2007/7 Information and communication technologies.* Paris: OECD.
OECD Directorate for Science Technology and Industry (2009). *The role of digital identity management in the internet economy: A primer for policy makers*. Paris: OECD.
Ogura, T. (2006). Electronic government and surveillance-oriented society. In D. Lyon (Ed.), *Theorizing Surveillance. The panopticon and beyond* (Vol. 2006, pp. 270-295): Willan publishing.
Olson, J. S., Grudin, J., & Horvitz, E. (2005). *A Study of Preferences for Sharing and Privacy*. Paper presented at the CHI'05 Extended Abstracts on ACM SIGCHI Conference on Human Factors in Computing Systems.
Palfrey, J., & Gasser, U. (2008). *Born Digital. Understanding the first generation of digital natives*. New York: Basic Books.
Patton, M. Q. (2002). *Qualitative research and evaluation methods* (3rd ed.). London: Sage.
Peckover, S., White, S., & Hall, C. (2008). Making and Managing Electronic Children: E-assessment in child welfare. *Information, Communication and Society, 11*(3), 375-394.
Pfitzmann, A. (2007). *An Introduction to Digital identity*. Paper presented at the OECD Workshop on Digital Identity Management, 8 May 2007. from http://www.oecd.org/dataoecd/6/63/38540119.pdf
Raab, C. D. (2005). Perspectives on "personal identity". *BT Technology Journal, 23*(4), 15-24.
Raab, C. D. (2007). The EGPA Study Group at 20: Reflections backwards, forwards, and sideways. *Information Polity, 12*(4), 219-226.
Regan, P. (1995). *Legislating Privacy*. Chapel Hill: University of North Carolina Press.
Ring, P. S., & Van der Ven, A. H. (1992). Structuring co-operative relations between organizations. *Strategic Management Journal, 13*, 483-498.
Ritter, H. W. J., & Webber, M. M. (1973). Dilemmas in a general theory of planning. *Public Sciences, 4*, 155–169.
Roberts, A. (2004). ORCON Creep: Information sharing and the threat to government accountability. *Government Information Quarterly, 21*(3), 249-267.
Rommel, J., & Christiaens, J. (2009). Steering from ministers and departments: Coping strategies of agencies in Flanders. *Public Management Review, 11*(1), 79-100.
Rotchanakitumnuai, S. (2008). E-Govsqual-risk:A model for measuring perceptions of e-government service value. *Business Process Management Journal, 14*(5), 724-737.
Schneier, B. (2004). Secret & Lies. Digital Security in a Networked World. Indianapolis: Wiley Publishing, Inc.
Schoeman, F. (1984). Privacy and Intimate Information. In F. Schoeman (Ed.), *Philosophical Dimensions of Privacy: An Anthology*. Cambridge: Cambridge University Press.
Smith, P., Smith, N., Sherman, K., Goodwin, I., Crothers, C., Billot, J., et al. (2010). The Internet in New Zealand 2009, World Internet Project New Zealand, from wipnz.aut.ac.nz
Solove, D. (2004). *The Ditigal Person: Technology and Privacy in the Information Age*. New York: New York University Press.

State Services Commission (2010). Kiwis Count 2009: New Zealanders' satisfaction with public services. Wellington: State Services Commission.

Statistics New Zealand (2010). The Source July 2010: Official Statistics News. Wellington: Statistics New Zealand.

Taylor, J., Lips, A. M. B., & Organ, J. (2006). Freedom with Information: Electronic Government, Information Intensity and Challenges to Citizenship. In R. A. Chapman, and M. Hunt (Ed.), *Freedom of Information: Perspectives on Open Government in a Theoretical and Practical Context*. Aldershot: Ashgate.

Taylor, J., M, L., & Organ, J. (2007). Information-Intensive Government and the Layering and Sorting of Citizenship. *Public Money & Management, 27*(2), 161-164.

Taylor, J. A., & Lips, A. M. B. (2008). The citizen in the information polity: Exposing the limits of the e-government paradigm. *Information Polity, 13*, 139-152.

Taylor, J. A., Lips, A. M. B., & Organ, J. (2009). Idenfitication Practices in Government: Citizen Suveillance and the Quest for Public Service Improvement. *Identity in the Information Society*. Retrieved from http://www.springerlinker.com/content/2p12731712732452/

Thomas, R., & Walport, M. (2008). Data sharing review report. United Kingdom: Her Majesty's Revenue and Customs (HMRC).

Torgler, B. (2007). Tax Compliance and Tax Morale: A Theoretical and Empirical Analysis. Cheltenham: Edward Elgar Publishing Limited.

Tsai, J., Egelman, S., Cranor, L., & Acquisti, A. (2007). *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*. Paper presented at the 6th Workshop on the Economics of Information Security (WEIS).

Van de Walle, S., Kampen, J. K., & Bouckaert, G. (2005). Deep Impact for high-impact agencies? Assessing the role of bureaucratic encounters in evaluations of government. *Public Performance & Management Review, 28*(4), 532-549.

Van de Walle, S., Van Roosbroek, S., & Bouckaert, G. (2008). Trust in the Public Sector: is There any Evidence for a Long-Term Decline? *International Review of Administrative Sciences, 74*(1), 47-64.

Van Dijk, J. A. G. M. (2005). *The Deepening Divide: Inequality in the information society*. London: Sage publications.

Varney, D. (2006). Service Transformation: A better service for citizens and businesses, a better deal for the taxpayer Available from http://www.hm-treasury.gov.uk/media/4/F/pbr06_varney_review.pdf

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information techology: Toward a unified view. *MIS Quarterly, 27*(3), 425-478.

Viseu, A., Clement, A., & Aspinall, J. (2004). Situating privacy online: Complex perceptions and everyday practices. *Information, Communication and Society, 7*(1), 92-114.

Wacks, R. (1989). *Personal Information: Privacy and the Law*. Oxford: Clarendon Press.

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

Wetmore, J. M. (2007). Distributing Risks and Responsibilities: Flood Hazard Mitigation in New Orleans. *Social Studies of Science, 37*(1), 119-126.

Yildiz, M. (2007). *E-government research: Reviewing the literature, limitations, and ways forward*.

Zureik, E. (2008). Summary of findings of International surveillance and privacy opinion research conducted under the Globalization of Personal Data Project. *The Surveillance Studies Centre*. Retrieved from http://www.sscqueens.org/research/intl_survey