Examining the Impact of E-privacy Risk Concerns on Citizens' Intentions to use E-government Services: An Oman Perspective

Dhiyab Salim Said Al Abri

This thesis is presented for the degree of Doctor of Philosophy of Murdoch University

2009
I declare that this thesis is my own account of my research and contains as its main content work which has not previously been submitted for a degree at any tertiary education institution.

Dhiyab Al Abri
Abstract

E-privacy concerns are among the online transactions risks that influence the use of e-services and e-government services. Whilst there have been studies that have analysed the impact of e-privacy on the willingness of people to utilize the Internet, especially in e-commerce, there has been limited research in relation to e-government services for a specific demographic group. This study has examined the impact of e-privacy risk concerns on the acceptance of e-government services in Oman using an integrated model. The model is based on Liu et al.’s (2005) privacy-trust-behavioral intention model, the broader technology acceptance literature, and recent work on e-privacy awareness and protection. The research used both quantitative and qualitative approaches: data collection by questionnaire and a series of semi-structured interviews. The sampling frame for the study was civil services government employees in Oman. The model was tested using partial least squares and the results were compared to those obtained from the interview data.

The study found that e-privacy awareness significantly impacts the level of e-privacy risk concerns. Social norms and perceived usefulness were found to play a significant role in influencing the intention to use e-government services. The study also found that e-privacy concerns and perceptions of the protection available against risks influence citizens’ intentions to use e-government services via their influence on the perceived trustworthiness of these services. Thus trustworthiness is a factor that could be an obstacle to successful e-government services project implementation. Therefore the thesis recommends that governments pay greater attention to the role of e-privacy concerns and put in place security and e-privacy controls. Citizens should then be made aware of these in order to build the required level of trust and confidence in these services.
# Table of Contents

## Chapter 1. Introduction

1.1. Background .................................................................................. 1
1.2. The problem statement ................................................................ 1
1.3. Research objectives and questions .............................................. 2
1.4. Significance of the study ................................................................. 4
1.5. Research approach ...................................................................... 5
1.6. The thesis outline ........................................................................ 6
1.7. Definition of key terms ................................................................. 8

## Chapter 2. Research Background

2.1. Introduction ................................................................................. 11
2.2. About Oman .............................................................................. 11
2.2.1. ICT vision and strategy .............................................................. 13
2.2.2. E-Oman mission .................................................................. 14
2.3. E-government services in Oman .................................................. 15
2.4. Growth of e-government status in Oman ...................................... 17
2.5. Internet privacy concerns in Oman .............................................. 18
2.6. Oman Internet privacy protection initiatives ............................... 21
2.7. Oman e-services awareness efforts ............................................ 23
2.8. Summary ..................................................................................... 24

## Chapter 3. Literature Review

3.1. Introduction ................................................................................ 26
3.2. E-services adoption and use background .................................... 26
3.2.1. E-privacy risk concerns ............................................................ 27
3.2.2. E-privacy protection ................................................................. 29
3.2.3. Trustworthiness of e-services .................................................. 32
3.2.4. E-privacy awareness ............................................................... 33
3.3. Behavioural models relevant to information technology use ....... 34
3.3.1. Main behavioural models ......................................................... 34
3.3.2. Key factors influencing system usage ...................................... 37
3.4. Factors impacting e-commerce services usage ........................... 39
3.5. Factors impacting e-government services usage ....................... 45
3.5.1. Previous experience ............................................................... 49
3.5.2. Perceived risks .................................................................. 50
3.5.3. E-privacy protection .............................................................. 50
3.5.4. Trust ................................................................................... 51
3.6. The role of culture in adoption of e-services ............................... 51
3.7. Summary .................................................................................... 54

## Chapter 4. Research Model

4.1. Introduction ................................................................................ 55
4.2. Research objectives and questions .............................................. 55
4.3. Constructs of interest ................................................................. 56
4.3.1. Perceived usefulness of e-government services ...................... 56
4.3.2. Social norms ...................................................................... 57
4.3.3. Prior e-services experience .................................................... 57
4.3.4. E-privacy risk concerns ........................................................ 57
4.3.5. E-privacy awareness .............................................................. 58
Chapter 5. Research Methodology

5.1. Introduction .................................................. 71
5.2. Triangulation of method ....................................... 71
5.3. Participants .................................................... 72
5.4. Development of the questionnaire ......................... 73
  5.4.1. Questionnaire design .................................. 73
  5.4.2. Questionnaire pre-testing ............................. 82
  5.4.3. Pilot study using questionnaire ...................... 83
5.5. Quantitative data collection procedures .................. 85
5.6. Qualitative data collection procedures .................... 87
5.7. Data analysis ................................................ 88
  5.7.1. Quantitative data analysis ........................... 89
  5.7.2. Qualitative data analysis ............................ 92
5.8. Summary .................................................. 94

Chapter 6. Quantitative Findings

6.1. Introduction .................................................. 96
6.2. Descriptive statistics ......................................... 96
  6.2.1. User profile ............................................. 96
  6.2.2. Use of e-government services ....................... 99
  6.2.3. Summary information on the research constructs .. 102
6.3. Testing the measurement model ......................... 103
  6.3.1. Convergent validity .................................. 104
  6.3.2. Discriminant validity ................................ 110
6.4. Test of the structural model .............................. 113
  6.4.1. Variance explained .................................... 114
  6.4.2. Assessment of path coefficients .................... 115
6.5. Hypotheses testing ......................................... 116
6.6. Assessment of relationships strength .................. 120
6.7. Assessment of total effects .............................. 121
6.8. Participants’ extra feedback .............................. 122
6.9. Summary .................................................. 123

Chapter 7. Qualitative Findings

7.1. Introduction .................................................. 125
7.2. Background information .................................... 125
7.3. Qualitative findings relating to research constructs .... 127
  7.3.1. Prior e-services experience ......................... 127
  7.3.2. Social norms .......................................... 128
  7.3.3. E-privacy risk concerns ............................. 129
  7.3.4. Perceived e-privacy protection .................... 131
  7.3.5. E-privacy awareness ................................ 134
  7.3.6. Perceived usefulness of e-government services .. 136
  7.3.7. Perceived trustworthiness of e-government services 138
  7.3.8. Intention to use e-government services ............ 141
7.4. Support for the research hypotheses ..................... 142

iv
# 7.5. Participants’ perceptions of e-government services success in Oman

Page: 149

# 7.6. Quantitative and qualitative findings

Page: 152

# 7.7. Summary

Page: 154

## Chapter 8. Discussion and Conclusion

Page: 155

### 8.1. Introduction

Page: 155

### 8.2. Model discussion

- **8.2.1. Role of social norms**: 157
- **8.2.2. Role of prior e-services experience**: 159
- **8.2.3. Role of e-privacy risk concerns**: 159
- **8.2.4. Role of perceived e-privacy protection**: 161
- **8.2.5. Role of e-privacy awareness**: 162
- **8.2.6. Role of perceived trustworthiness of e-government services**: 163
- **8.2.7. Role of perceived usefulness of e-government services**: 165

### 8.3. Answering the research questions

Page: 165

### 8.4. Research limitations and research implications

- **8.4.1. The research limitations**: 168
- **8.4.2. The research implications**: 169

### 8.5. Recommendations for the Omani government

Page: 171

### 8.6. The research conclusion

Page: 173

### Appendix A: English version of the questionnaire

Page: 176

### Appendix B: The Arabic version of the questionnaire

Page: 187

### Appendix C: The interview guide

Page: 200

### Appendix D: Themes selection process

Page: 205

### Appendix E: Interviewees’ feedback vs. research constructs

Page: 209

### Appendix F: Participants’ responses summary

Page: 213

### Appendix G: Interview data vs. research hypotheses

Page: 216

### Appendix H: List of measurement items

Page: 221

### References

Page: 225

### Publications arising from this research

Page: 239
List of Figures

Figure 2.1 Map of Oman (WorldAtlas.com) ................................................................. 12
Figure 2.2 Towards e-Oman ....................................................................................... 13
Figure 3.1 TAM (Davis, 1986) .................................................................................. 35
Figure 3.2 TAM2 (Venkatesh & Davis, 2000) .............................................................. 36
Figure 3.3 UTAUT (Venkatesh et al., 2003) ................................................................. 37
Figure 3.4 E-CAM (Lee et al., 2001) ......................................................................... 40
Figure 3.5 Privacy-Trust-Behavioral Intention Model (Liu et al., 2005; Liu et al., 2004) ........................................................................................................................................ 42
Figure 3.6 AB2CEWS acceptance model (Kim et al., 2009) .......................................... 43
Figure 3.7 Malhotra, Kim and Agarwal’s research model (2004) ................................. 44
Figure 3.8 E-government Adoption Model (Warkentin et al., 2002) ........................... 47
Figure 3.9 Carter and Belanger’s research model (2005) .............................................. 48
Figure 3.10 Trust and risk in e-government adoption (Belanger & Carter, 2008) ............ 49
Figure 4.1 The research model tested in this study ...................................................... 63
Figure 6.1 The measurement model ............................................................................ 104
Figure 6.2 Hypotheses tested ..................................................................................... 114
Figure 6.3 Structural model ....................................................................................... 117
Figure 8.1 The final model showing supported relationships ..................................... 156
## List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-1</td>
<td>Oman e-government services</td>
<td>16</td>
</tr>
<tr>
<td>4-1</td>
<td>Construct definitions</td>
<td>61</td>
</tr>
<tr>
<td>4-2</td>
<td>Summary of the research hypotheses</td>
<td>69</td>
</tr>
<tr>
<td>5-1</td>
<td>Background and demographic items</td>
<td>75</td>
</tr>
<tr>
<td>5-2</td>
<td>Perceived usefulness items</td>
<td>75</td>
</tr>
<tr>
<td>5-3</td>
<td>Items to measure social norms</td>
<td>76</td>
</tr>
<tr>
<td>5-4</td>
<td>Items to measure prior e-services experience</td>
<td>77</td>
</tr>
<tr>
<td>5-5</td>
<td>Items to measure e-privacy risk concerns</td>
<td>78</td>
</tr>
<tr>
<td>5-6</td>
<td>Items to measure e-privacy awareness</td>
<td>79</td>
</tr>
<tr>
<td>5-7</td>
<td>Items to measure perceived e-privacy protection</td>
<td>79</td>
</tr>
<tr>
<td>5-8</td>
<td>Items to measure perceived trustworthiness of e-government services</td>
<td>80</td>
</tr>
<tr>
<td>5-9</td>
<td>Items to measure intention to use e-government services</td>
<td>81</td>
</tr>
<tr>
<td>5-10</td>
<td>Items to measure actual use</td>
<td>82</td>
</tr>
<tr>
<td>5-11</td>
<td>Pilot construct validity</td>
<td>85</td>
</tr>
<tr>
<td>5-12</td>
<td>Questionnaire distribution</td>
<td>86</td>
</tr>
<tr>
<td>5-13</td>
<td>Criteria used for convergent validity</td>
<td>90</td>
</tr>
<tr>
<td>6-1</td>
<td>Age distribution</td>
<td>97</td>
</tr>
<tr>
<td>6-2</td>
<td>Educational background</td>
<td>98</td>
</tr>
<tr>
<td>6-3</td>
<td>Internet and e-service background</td>
<td>98</td>
</tr>
<tr>
<td>6-4</td>
<td>Previous ICT training</td>
<td>99</td>
</tr>
<tr>
<td>6-5</td>
<td>Level of e-government services use</td>
<td>99</td>
</tr>
<tr>
<td>6-6</td>
<td>Period of e-government services usage</td>
<td>100</td>
</tr>
<tr>
<td>6-7</td>
<td>E-government services usage in hours</td>
<td>100</td>
</tr>
<tr>
<td>6-8</td>
<td>Personal information disclosure and payment</td>
<td>101</td>
</tr>
<tr>
<td>6-9</td>
<td>Amount paid online for government services</td>
<td>102</td>
</tr>
<tr>
<td>6-10</td>
<td>Construct summary information</td>
<td>103</td>
</tr>
<tr>
<td>6-11</td>
<td>Initial outer loading values</td>
<td>105</td>
</tr>
<tr>
<td>6-12</td>
<td>Outer loadings final values</td>
<td>106</td>
</tr>
<tr>
<td>6-13</td>
<td>Outer loading bootstrap analysis</td>
<td>109</td>
</tr>
<tr>
<td>6-14</td>
<td>Convergent validity measures</td>
<td>110</td>
</tr>
<tr>
<td>6-15</td>
<td>Table of cross loadings</td>
<td>112</td>
</tr>
<tr>
<td>6-16</td>
<td>Discriminant validity</td>
<td>113</td>
</tr>
<tr>
<td>6-17</td>
<td>R square values</td>
<td>115</td>
</tr>
<tr>
<td>6-18</td>
<td>Significance of path coefficients</td>
<td>116</td>
</tr>
<tr>
<td>6-19</td>
<td>Total effects</td>
<td>121</td>
</tr>
<tr>
<td>7-1</td>
<td>Background information about interviews</td>
<td>126</td>
</tr>
<tr>
<td>7-2</td>
<td>Consistency of interview findings with hypotheses</td>
<td>148</td>
</tr>
<tr>
<td>7-3</td>
<td>Consistency between results of quantitative and qualitative analyses</td>
<td>153</td>
</tr>
</tbody>
</table>
Acknowledgments

I would like to start by greatly thanking God for giving me the strength and willingness to overtake this work. I would next like to thank my supervisors Associate Professor Tanya McGill and Dr. Michael Dixon for their incredible assistance and guidance. They were always available for consultations and proof reading my drafts and guiding me with their practical critiques.

A special thanks to Associate Professor Tanya McGill, the person I learnt a lot from and relied on for her experience and expertise. Also she was a great help with my English and the encouragement source for me to always go forwards. I am so fortunate to have a supervisor like her; she is indeed a truthful companion in my PhD thesis journey.

I would like to thank my lovely wife Aisha Al Yarabi for being very supportive and patient with me during my most difficult times. I thank her for travelling with me all the way to Australia and staying abroad with me for the last four years. Her love, understanding and hard work enabled the family and I to make the educational journey successfully.

I would like thank the rest of my family here in Perth including my great sons Mataz, Malik, and Salim and my three most beautiful daughters Noor, Noha, and Shadha for being so considerate and to work out the culture shock and the language challenges just to be with their dad. The thanks also continues to my family back home in Oman. In particular, the greatest mom and dad of mine who without their plusses and prayers I would not have done it.
I would also want to thank everyone who helped me to make the journey successfully, especially Gillian Ajayi at Murdoch International Office and the rest of the international office team, His Excellency Hamad Al Hajri the General Consular at the Omani Consulate in Australia and his most supportive team, the Omani student society in Western Australia for providing us the warm Omani social environment in Perth, the Omani Ministries of Higher Education and Civil Service for sponsoring my PhD scholarship. A special thanks to my bosses at my work for giving me the chance to make my PhD dream become true.

I would like to dedicate this thesis to my family in particular mom and dad for not only bringing me to life but putting their hands with me to be stronger. My mom and dad will forever continue to shape my life through values and great inspiration. My family will be the best there ever was.
Chapter 1. Introduction

1.1. Background

The recent huge expansion in use of the Internet has increased the risk to online information privacy (e-privacy). It is difficult for people to know where their information is stored, or who might be using it. Therefore protecting online privacy is a real challenge. E-privacy and trust issues have been shown to influence willingness to be involved in Internet transactions relating to money and personal, sensitive information (Metzger, 2004; Olivero & Lunt, 2004). These issues apply to both e-commerce and e-government projects.

Oman has been implementing a plan to establish the Oman e-society vision since 2003 (Information Technology Authority, 2006b). This plan includes an e-government project, which is intended to facilitate Omani society by supporting most commercial, political, and social online transactions and services. The research described in this thesis concerns the potential impact of e-privacy issues on citizens’ usage of e-government services in Oman.

1.2. The problem statement

This study defines e-government, as it is defined by the Omni authorities, to be the use of information technology and communication infrastructure ability by government units to transform relations with citizens, and businesses electronically. The study defines an e-government service as any service that is made available by the government via the Internet to save time and make citizens’ lives more convenient; for
example in Oman one such service is *Higher Education Admissions Online*


While e-government has played an important role in the expansion of the Internet across the globe within both the public and private sectors, there has been insufficient empirical research concerning its adoption and use by Internet users (Metzger, 2004). Acceptance problems have occurred in many commercial and government projects across the world (Lee & Rao, 2005; Liu, Marchewka, Lu, & Yu, 2005; Metzger, 2004; Olivero & Lunt, 2004). Dinev and Hart (2006b) believe that there are two main dimensions of e-privacy concerns among Internet users; these are concerns related to unauthorized access or interception of users’ personal information and concerns related to the possible misuse of such information. These two main issues could deter online users from using the services or lead to them not giving complete and accurate personal data.

The research described in this thesis assumes that Oman’s e-government project will be subject to the e-privacy concerns of citizens and that such issues might discourage citizens from using the e-government services. Little research into the adoption of e-government services has taken place in the Arab world; therefore this implementation provides an excellent opportunity to broaden the contexts in which e-government adoption has been studied.

### 1.3. Research objectives and questions

Many researchers have considered e-privacy to be a key factor of concern among online users and many believe that it might become one of the most important barriers to e-services development (Dinev, Bellotto, Hart, & Russo, 2006; Dinev & Hart, 2006b;
Liu et al., 2005; McDonagh, 2002; Metzger & Docter, 2003; Suh & Han, 2003; Vijayasarathy, 2004; Yu, 2005).

E-government users, as in any other technology adoption, weigh the perceived benefits and risks before using the technology (Horst, Kuttischreuter, & Gutteling, 2007). E-privacy risks are considered as an increasingly important hazard associated with using e-government services (Ackerman & Mainwaring, 2005; Belanger & Carter, 2008; Lau, 2003; Srivastava & Teo, 2005; Warkentin, Gefen, Pavlou, & Rose, 2002). Therefore, citizens’ e-privacy risk concerns are a potential obstacle to e-services growth and an important issue to both individuals and government organizations.

This study focuses on the government services provided online to citizens. The primary objective of the research described in this thesis is to examine the impact of online privacy concerns on citizens’ acceptance of e-government services (government services to citizens). It also considers the impact of information security and users’ ability to trust e-government services, given their privacy concerns.

The research objectives were addressed through answering two high level research questions. These questions are as follows:

- Do e-privacy risk concerns influence citizens’ intentions to use e-government services in Oman?
- What other factors related to e-privacy influence citizens’ intentions to use e-government services in Oman?
1.4. **Significance of the study**

According to Carter and Belanger (2005) successful e-government project adoption depends heavily on citizens’ acceptance of the services and the level of trust they have in the new services. Warkentin et al. (2002) found that culture influences this acceptance. Oman is one of the Islamic countries in the Middle East that preserves Islamic culture. Digitizing government services could be resisted due to lack of trust and concerns about privacy risks. These issues suggest the importance of examining the impact of e-privacy risk concerns on the use of e-government services in Oman and the similar countries. For that reason this research focuses on the e-privacy concerns and trust of citizens who are intended to use the e-government services in Oman. There is no research that has specifically tackled such an issue in Oman before. Whilst there have been many studies elsewhere that have analysed the impact of Internet privacy on the willingness of people to utilize the Internet, especially in e-commerce, no one has categorized the concern factors in relation to a specific demographic group (the Omani) with a view to implementing an e-government project, nor have they proposed such a comprehensive model of the factors proposed to influence e-government adoption.

Specifically the research makes the following three significant contributions to scholarly knowledge about the adoption of e-government services:

1. E-commerce and e-government have many differences such as the fact that businesses engaging in e-commerce can choose their customers, but e-government services should be provided to the entire eligible population. Also with e-government, the government is obliged to allocate resources and provide the service in the best interests of the citizen, however e-commerce can focus on profits (Carter and Belanger, 2003). Most previous studies have focused on the
e-commerce domain and very few studies have examined the issues in relation
to e-government services adoption and use. This study addresses this lack.

2. Though there are a number of studies that have emphasized the importance of
studying e-privacy risk concerns and their role in influencing citizens’ trust of
e-government services (e.g. Belanger & Hiller, 2006; Jho, 2005; Kim, 2008; Yu,
2005), few of them have clearly established the relationships between the
different factors believed to influence the use and adoption of e-government
services. This study has established the roles of social norms, e-privacy
awareness, e–privacy risk concerns, prior experience and level of trust in
e-government services in the adoption process.

3. This research provides a deeper understanding of the role of e-privacy concerns
in the adoption of e-government projects not only in Oman but in other countries
of a similar demographic nature.

1.5. Research approach

To answer the research questions, a model of the role of e-privacy in the adoption of
e-government services was proposed and tested. A survey data collection approach was
chosen. The research involved both quantitative and qualitative approaches: data
collection by questionnaire and a series of semi-structured interviews. The data was
collected in Oman over about two months. The sampling frame for the study was civil
services government employees in Oman. This sector is considered to be the largest
national sector in terms of its number of employees, with more than 110,000 employees
(Ministry of Civil Service, 2007). The employees were asked to express their views as
citizens not as government employees.
Construct measurement for the quantitative part of the study was based on previous studies with minor re-wording to suit the e-government domain. Partial least squares (PLS) was used to test the model.

The qualitative part of the research was used to compliment the quantitative findings. Interviews were undertaken with potential e-government users (consistent with the quantitative data collection) and with government executive personnel e-services experts, and e-government project personnel. Insights from the literature review formed the basis of the interview questions. The responses were inspected for statements that addressed the relationships contained in the research model. These statements were then classified into general themes representing the relationships of interest. The themes were permitted to emerge from the data. A multiple classification scheme was used so that each remark could be classified into more than one category.

1.6. The thesis outline

The thesis is organized in eight chapters. This chapter provides general background followed by the aims and objectives of the research. It also introduces the research methodology and provides a description of the thesis structure and definitions of key terms.

Chapter 2 presents an overview of Oman and the use of e-government services in Oman. It also provides an overview of the current status of plans to develop and improve the information technology and communications (ICT) sector and e-government services in the country. In addition it presents background research on e-privacy concerns and e-privacy security efforts in Oman.
Chapter 3 reviews the literature on technology adoption in general and e-commerce and e-government adoption in particular. It explores the factors that may influence e-government adoption with an emphasis on those relating to e-privacy. The models reviewed in this chapter form a basis for the development of a model of the role of e-privacy in the adoption of e-government services.

Chapter 4 introduces the research model. It describes the proposed constructs, model, and the research hypotheses.

Chapter 5 describes the research methodology used in the study. The chapter presents an overview of the methodology and the rationale behind the choice. The chapter also describes the data collection methods and the choice of participants. It also provides an overview of the data analysis approaches.

Chapter 6 and Chapter 7 report the results of the study. Chapter 6 reports the results of the quantitative data collection and analysis. The results of the measurement model and structural model analyses are presented. The chapter concludes by presenting the results of the testing of the hypotheses. Chapter 7 reports the results of the qualitative data collection and analysis. It also provides a brief comparison of the quantitative and qualitative findings.

Chapter 8 presents a discussion of the research results and the implications of the study for research. It also discusses the limitations of the study and provides recommendations to the Omani government. The chapter then presents the research conclusion that summarizes the research main points.
1.7. **Definition of key terms**

This section defines the key variables and terms that are used throughout the thesis:

**Discriminant validity** tests that each measurement item correlates weakly with all other constructs except for the one with which it is proposed to be associated.

**E-government** is the use of information technology and communication infrastructure ability by government units to transform relations with citizens and businesses electronically.

**E-government service** is any service that is made available by the government via the Internet to the citizens, businesses, and government units.

**E-Oman** is an Omani project that comprises a wide range of initiatives and services that are designed and created to improve the efficiency of government services, enhance the activities of businesses and empower individuals with skills and knowledge, to meet society’s needs and expectations and to direct Oman towards becoming a sustainable knowledge-based economy.

**E-privacy** is the claim of individuals that their online personal data should generally not be available to others without their prior consent and approval.

**E-privacy awareness** relates to how much citizens know about online e-privacy risks and about related issues such as how to protect themselves and what protection is provided by service providers.
E-privacy risk concerns are citizens’ concerns regarding potential loss of control over personal information, such as when information about a citizen, obtained during their use of e-government services, is used without permission.

E-service is a service provided via the Internet that assists users to complete tasks or conduct transactions. Therefore, e-services encompass numerous sectors of social and public life, including information retrieval, e-commerce, e-learning, financial services, and e-government.

Information and communications technology (ICT) is a broad term. In this thesis the term is used specifically with respect to the leveraging of information technology and communications to provide Oman with the foundation for electronic services.

Intention to use e-government services relates to an individual’s willingness to use e-government services sites.

Measurement model is a sub model of PLS that specifies the indicators for each construct and assesses the reliability of each construct to predict the causal relationships.

Partial Least Squares (PLS) is a tool to examine unobservable variables (constructs) in relation to the proposed observable variables (indicators). PLS was used to determine the relationships among the variables of the proposed model.
Perceived e-privacy protection is the degree to which a citizen believes that facilitating conditions (technical, organizational) exist that can protect his/her online privacy while using e-government services.

Perceived trustworthiness of e-government services relates to citizens’ perceptions of the integrity of e-government services and the extent to which they can be trusted.

Perceived usefulness is the degree to which a citizen believes that using a particular e-government service would enhance his or her ability to obtain information and conduct transactions with the government.

Prior e-services experience is the extent of previous hands on experience with online services that a citizen has had.

Social norms are the rules for the way in people should act in a group or society. A person may be more likely to perform a particular behaviour, in this case to use e-government services, if it is the social norm, established by family members, friends, co-workers and supervisors at work.

Structural equation modelling is a multivariate data analysis technique used to estimate a series of interrelated dependence relationships simultaneously.

Triangulation of methods mixes quantitative and qualitative data collection approaches to maximize the strength of the collected data.
Chapter 2. Research Background

2.1. Introduction

This chapter describes the research location and provides general background information about Oman. The country profile in Section 2.2 gives a snap shot description of the Oman ICT vision and strategy: e-Oman mission. Section 2.3 shines light on Oman e-government services. E-government services in Oman were considered as a portion of e-Oman vision. Section 2.4 describes e-privacy concerns in Oman. Some of the nearby countries’ e-privacy concerns are also noted. Section 2.5 discusses e-privacy protection initiatives in Oman. Non technical and technical security solutions in Oman are also described. Section 2.6 is on the Omani e-services awareness efforts. The section describes the plans and the practices proposed to develop the required ICT skills and awareness within the Omani society.

2.2. About Oman

Oman is the third largest country in the Arabian Peninsula after the Kingdom of Saudi Arabia and the Republic of Yemen. As shown in Figure 2.1 Oman is situated in Southwest Asia, located between the Arabian Sea, the Gulf of Oman, and the Arabian Gulf (Persian Gulf) (WorldAtlas.com). According to the most recent government figures, the total estimated population of Oman is 2.341 million people (Ministry of National Economy, 2006). Oman has a land area of about 309.5 thousand square kilometres and a coastline of 1700 kilometres.
The Internet in Oman is relatively new as it was only introduced in 1997; however it has already started impacting most sectors of the economy and society. Nowadays, Omani people are increasingly using online government and businesses services. The number of Internet users in Oman has been dramatically increasing to reach 112,000 subscribers in 2008 (“More than 2 million subscribers in Omantel and Oman mobile by last June 08”, 2008). A study 2004 by Al-Sabbagh and Molla found that in Oman the Internet users were mainly young, educated, and employed and were about 60% male and about 40% female (Al-Sabbagh & Molla, 2004).

Oman enjoys a stable political, economic and social system. The stability that Oman has enjoyed over the last four decades has provided an opportunity for the Sultanate to realise its aspirations in social, economic and political spheres. Oman is a middle-income economy. The Omani national economy mainly depends on oil and gas resources. Oman also continuously seeks to attract foreign investment in the fields of higher education, tourism, and the information technology (Central Intelligence Agency, 2009).
2.2.1. **ICT vision and strategy**

Under the direction of his majesty Sultan Qaboos – Sultan of Oman, Oman has made transformation technology a national priority since the early 1970s. In 1995 Oman launched a national long term plan, ‘Oman 2020’ (1996-2020) which focuses on ICT side by side with other economical and social aspects. As shown in Figure 2.2, a great deal of attention was given to ICT to establish the major fundamentals of a knowledge based economy, in an effort to increase the productivity of the Omani economy and improve citizens’ livelihood. Knowledge based society, as viewed by the government of Oman, is society in which the government operations and information is made accessible to all society sections transparently, efficiently, and is regularly updated. The plan also aims to bring out the society’s potential strengths to participate in advancing Oman by building the required skills and transforming the society using enhanced ICT capabilities (Information Technology Authority, 2006a).

![Figure 2.2 Towards e-Oman](image)

By leveraging ICT plans and projects Oman wishes to provide the country with a knowledge-based economy that is considered to be the major essential force driving the economy. For that, since May 7, 2003 Oman has been implementing a plan to establish the Oman e-society vision, which is meant to facilitate the Omani society by supporting
most commercial, political, and social online transactions and services. As part of this
Oman is targeting the following major objectives (Information Technology Authority,
2002):

- Laying down a digitized network all over the country;
- Expanding the range and number of information technology industries;
- Creating a supportive environment for e-business and e-commerce;
- Streamlining e-government services to citizens and businesses;
- Creating an information security infrastructure.

Through the ICT vision Oman is hoping to achieve sustainable national economic
development and to facilitate the public sector, private sectors and private citizens with
electronic collaborative services. In particular, in 2006-2010 Oman is planning to put a
strong emphasis on developing the ICT sector by implementing a phased digital strategy
concentrating on building the foundation for electronic service delivery and allocating
special priority to information technology research and development work (Ministry of
National Economy, 2006).

2.2.2. \textit{E-Oman mission}

Digital Oman (e-Oman) is an e-governance national initiative that has been proposed
based on his majesty Sultan Qaboos’ vision to create a knowledge based society in
Oman. The e-Oman initiative is spearheaded by the Information Technology Authority
(ITA) which was set up by the Royal Decree 52/2006 promulgated on May 31, 2006.
E-Oman is intended to establish efficient government-community-citizen ICT
infrastructure and provide better streamlined government services to the people of
Oman through the utilization of the Internet.
The main mission of e-Oman is to transform citizens, residences, visitors, business enterprises, and government entities in Oman to a knowledge based society. E-Oman is also intended to provide a wide range of convenient, cost effective, customer-oriented e-services to empower the people of Oman and to make their lives better (Information Technology Authority, 2007b).

2.3. E-government services in Oman

E-government as defined by the Omani ITA is the process of seamlessly integrating all ministries and government entities in Oman to provide faster and more effective online public services. It is to facilitate better interaction between citizens, businesses and government (Information Technology Authority, 2005).

The aims of e-government in Oman are to facilitate the citizens with better delivered services, to improve interactions with business and industry, and to empower citizens through more efficient access to information and better government management. In particular the Omani e-government is targeting the following (Information Technology Authority, 2007a):

- Streamlining government processes and introducing online transactions;
- Interconnecting government departments and units electronically to share common information for better governance;
- Creating a single e-government portal to save citizens’ time and money.

Oman is currently in the initial stages of establishing a single e-government services portal that aims to deliver e-government services in a more reliable and efficient manner. The portal is intended to be the main entry point for accessing government information and services. Access to the portal is not limited to Internet web access but
it provides for various access channels such as mobile phones and small screen handheld devices. The portal has been designed to enable a single strong authentication process. The portal is expected to provide online service delivery like downloadable e-forms along with online filling and submitting government forms (Information Technology Authority, 2007b).

The Omani e-government services portal will be linked electronically with the other government ICT initiatives such as e-legislation, e-tendering, e-payment framework, one-stop-shop (companies’ registrations and licensing), national identification registry, and a socio-economic database system (Information Technology Authority, 2009a). According to the ITA official site, a number of e-services do now exist in Oman and they are listed in Table 2.1 (Information Technology Authority, 2009b).

Table 2-1 Oman e-government services

<table>
<thead>
<tr>
<th>E-service description</th>
<th>E-service description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Offense Enquiry</td>
<td>Visa Status Enquiry</td>
</tr>
<tr>
<td>Online Visa Application</td>
<td>Lost Documents</td>
</tr>
<tr>
<td>Donations Portal For Charitable Organizations</td>
<td>Ministry of Finance Application For Supplier Code</td>
</tr>
<tr>
<td>Ministry of Regional Municipalities Services Forms</td>
<td>Case Enquiry</td>
</tr>
<tr>
<td>Researcher job / employers</td>
<td>Online Tenders</td>
</tr>
<tr>
<td>Smart Forms</td>
<td>E-payment Gateway</td>
</tr>
<tr>
<td>Higher Education Admission</td>
<td>Educational Portal</td>
</tr>
<tr>
<td>Monthly Statistical Bulletin</td>
<td>One-Stop Shop</td>
</tr>
<tr>
<td>Muscat Real Estate Directory</td>
<td>Birth Registration</td>
</tr>
<tr>
<td>MM Muscat Commercial Directory</td>
<td>Marriage Registration</td>
</tr>
<tr>
<td>Muscat Securities Market Watch</td>
<td>Omani ID Card</td>
</tr>
<tr>
<td>Dhofar Municipality Building Permit</td>
<td>Resident Card</td>
</tr>
<tr>
<td>Death Registration</td>
<td>Divorce Registration</td>
</tr>
</tbody>
</table>
2.4. **Growth of e-government status in Oman**

In 2003 when Oman launched its e-society plan, the United Nations Economic and Social Commission for Western Asia (ESCWA) classified Oman among the countries that have only partially utilized ICT in business to business, business to consumer, and e-commerce applications (ESCWA, 2003). They advised Omani decision makers to provide more support for adopting adequate technology, improving consumers’ e-society awareness, and building further trust in using the Internet. They also stated that a number of actions were recommended to give e-business more freedom and to provide more protection of personal privacy on the Internet (ESCWA, 2003).

In 2005 ESCWA again classified Oman among the lowest users of ICT, side by side with other ESCWA members: Bahrain, Kuwait, Egypt, and Qatar. They described Oman as having some ICT policies and strategies and a national vision in place along with some operational implementation plans and initiatives, however stated that Oman needed more efficient implementation plans and more practical initiatives (ESCWA, 2005).

In 2008 ESCWA stated that Oman had made some progress in the area of ICT social usage, as had many other ESCWA members. They believed that Oman should be more active in having more precise ICT indicators. Specifically, ESCWA stated the following (ESCWA, 2009):

- ICT sector/ICT goods statistics are practically nonexistent;
- Egypt and Jordan are more advanced than the other ESCWA Members;
- Recognition of the importance of ICT indicators at decision making level is still weak.
In March 2008 ESCWA assigned an advisory service to the Ministry of National Economy and the ITA of Oman to:

- Provide technical assistance for identifying the data required for building the relevant ICT indicators;
- Explore existing data and assist in devising data collection strategies for additional data required for the purpose;
- Provide technical assistance for framing questionnaire modules, instructions for data collection, and output table format.

In April 2009 at the World Economic Forum Oman was ranked in the 50th position out of 134 countries in the Global IT Report 2008-09 (Dutta & Mia, 2009). According to the report Oman has improved its ICT readiness ranking from 53rd in the 2007-08 report to its current place. Oman was also placed in the 22nd position for its efforts in procuring advanced technology products for its ICT systems and 39th in the government readiness index. The report also placed Oman in the 45th position for the government’s success in ICT promotion, availability of government services online, presence and efficient use of ICT within the public sector and e-participation.

2.5. **Internet privacy concerns in Oman**

In the past the Omani people normally only had to provide their personal information to well known and trusted people. However, today with growing use of the Internet and with government and local companies’ online systems becoming accessible by external parties, Omani citizens have started to become concerned about their information.

According to Gartner, the national e-society vision consulting firm, “The public must be made aware of the benefits, the fears must be addressed and participation encouraged”
Gartner views the public as the main stakeholder in the country’s ICT national project and therefore they have encouraged the government to enhance public confidence in the Internet by establishing the required steps toward Internet privacy, security, and confidentiality of information (Gartner, 2002a).

Gartner also notes that “Privacy and security are uncomfortable bed fellows – the Internet increases the problem” (Gartner, 2002a), and assumes that Internet users in Oman are not yet aware of appropriate and inappropriate online usage; nor do they know what to do when they encounter a security problem (Gartner, 2002a). Information security and e-privacy is considered to be the second most important concern in adopting e-government services in Oman. For example, in a study by Jabar and Razooki (2005) 86 out of 91 Omanis listed e-privacy as their major concern and were worried about using the Internet for their regular purchasing and other usage. Also 79 out of 85 people had no trust in general online transactions, and 77 out of 90 people were not willing to disclose their personal information to websites. These findings suggest that e-privacy could be a major obstacle to e-Oman.

In 2007 ESCWA scored Oman one out of five in terms of Internet privacy security readiness (ESCWA, 2008). The score reflects the fact that Oman had a very low level of achievement in building online services, in terms of the confidence the services instilled in the users and the level of security. Bahrain is a nearby country to Oman and an ESCWA member which was ranked higher than Oman in terms of Internet privacy protection readiness by ESCWA. However on Sunday September 3, 2006 Alarabiya.net (2006), reported that Bahrain has suffered many hacker attacks. The report stated that it was dangerous for the country to use the Internet in the coming election. The report used the last three months rate of hacker attacks to defend its view. The report noted
that there was at least one hacker attack per month on government sites occurring in Bahrain. Therefore the report suggested that it would be an enjoyable day for the hackers if Bahrain were to use the Internet for the November 2006 election because hackers might amass the transmitted data and break individuals’ information privacy. Moreover, the report speculated that the government might use the Internet to fake the voting result for its own benefit as there would be no proof of false results. The report also stated that most computer users generally acknowledge the security lack in the Internet and that the level of privacy is even worse. Therefore if that is the case in Bahrain what could it be in Oman?

According to a recent ESCWA report, none of the ESCWA members have effective Internet privacy protection measures (ESCWA, 2008). ESCWA also believes that what data security measures and online privacy policies there are in ESCWA countries are very basic when compared to international measures, so they recommend that more attention should be paid to these issues. Therefore ESCWA (2008) recommends the following:

- Accelerating the process of devising laws to counter misuse of ICT;
- Ensuring transparency in reporting incidents related to networks and database hacking;
- Increasing awareness campaigns on the different types of cyber crimes, to help ICT users avoid them;
- Increasing international and regional cooperation in fighting ICT crimes;
- Putting in place the highest security measures for local networks and computer systems connected to the Internet, especially in public sector organizations, to patch security holes and decrease the chances of attacks;
- Devising and publishing online privacy policies on every website.
2.6. **Oman Internet privacy protection initiatives**

This section describes the Internet privacy protection readiness of Oman. The section also presents the Internet privacy and initiatives that Oman has taken in the period between 2006 and now.

In 2002 Gartner drafted an information security management framework document for Oman (Gartner, 2002b). The framework is part of the overall ITA standards framework and is based on a structured collection of independent guidelines such as ISO 2700. It also provides processes and practices descriptions to ensure the protection of automated information assets from unauthorized access. Both business and government organizations can implement the framework in ways they choose to the best interest of the country and their consumers’. ITA plays an advisory role to those organizations that wish to implement the framework. Gartner recommends the full implementation of the framework to build up citizens’ confidence and as a way to a successful e-Oman adoption. In particular ITA (2009a) stated that the security framework aims to:

- Reduce internal and external security breaches;
- Create confidence among staff and clients when running business operations;
- Measure the effect that a security incident has when it does occur;
- Respond to an incident and minimize business damage;
- Ensure continuous improvement in information security processes;
- Ensure compliance with national rules, laws and regulations.

In 2003 due to the absence of specialized e-law, The Omani Retribution Law (Royal Oman Police, 2009) was amended and used as the Internet legislation in Oman. This law was drafted and implemented by the Royal Oman Police. It is used by law

21
enforcement in regulating Internet related activities. Article number 276 of this law describes the penalty consequences of the following actions:

- Distribution of online data without owner approval;
- Unauthorized access to electronic data and information;
- Spying on or retrieving information of another.

The penalties vary from 3 months to 3 years prison with a financial fine that can reach up to AUD $3000. This law has also been made available to the public on the Royal Oman Police site under their section ‘Regulation’ (Royal Oman Police, 2009).

According to ESCWA, until late 2006 Oman was not the only member that did not have comprehensive e-law and legislation, neither did most of the countries surrounding Oman such as Bahrain, Saudi Arabia, Kuwait, and Qatar. Therefore these countries should provide substantial legal protection for all online users. Having e-legislation for all sorts of electronic transactions is required and it has to be initiated in Oman (ESCWA, 2008).

On May 17, 2008 Oman launched the Omani national e-transactions law. The law is a comprehensive Internet governance document produced with the help of the McKenzie Consultancy firm. The new law is designed to create a balance between United Nations Internet law compliance and the Omani national requirements. The new law is expected to increase trust in the Internet. This law defines, in a comprehensive manner, the rules of dealing with online information processing and personal data collection within or between community institutions (ESCWA, 2008).

The Omani e-transactions law addresses key issues such as: validity of e-transactions, intellectual property protection, taxation and data protection, legal recognition for
electronic signatures, admissibility and evidential value of data messages, electronic payment validity and jurisdictional matters, issues of electronic messages and protection for privacy and security (ESCWA, 2008; Information Technology Authority, 2008).

### 2.7. Oman e-services awareness efforts

The Omani ITA executives strongly believe that the success of the e-Oman initiative depends on the citizens’ e-services awareness level and on how Omani society is prepared and empowered to transition in accordance with the National ICT strategy. Therefore a number of initiatives to promote skills development have been launched in partnership between the public and the private sector. Along with ICT training projects the ITA has launched a number of specialized awareness seminars and workshops on a monthly basis to introduce e-Oman and e-government to the general public. The e-Oman awareness and promotion campaign was launched on April 15, 2007 and includes a number of regional and global seminars and workshops to spread the understanding of the e-Oman concept and to highlight the importance of participation of all sectors and to call for foreign information technology investments (Information Technology Authority, 2006a).

Digital Oman Magazine (http://www.digitaloman.com) is another source that Oman is using to increase the ICT awareness level in Oman. This magazine is a quarterly periodical that was launched in April 2005 in cooperation with ITA and other government and private firms. The magazine was published by the Oman Establishment for Press, News, Publication and Advertising (OEPNPA) in co-operation with ITA. It is created to provide insights into the latest ICT news locally and internationally and to provide the local community with awareness of e-Oman and e-government progress and achievements. It is available electronically at the above
mentioned link in both English and Arabic language (Information Technology Authority, 2007c).

Government IT Training and Certification Project is an ICT awareness initiative in Oman which aims to minimize ICT literacy among the civil service employees. The project is to train more than 100,000 employees on the fundamental computer and Internet skills. That includes the use of word processing applications and dealing with networks and the Internet including electronic mail and various Internet risks. These programs are provided by well known ICT program providers in the country. The project duration is 2008 to 2011 (Information Technology Authority, 2007c).

Although these efforts are helping to make the people of Oman aware of the e-Oman vision, they are not yet addressing awareness of Internet privacy issues adequately nor do they address online risk perceptions (Information society portal for the ESCWA region, 2008). Therefore Oman needs to make further efforts to provide privacy and security awareness campaigns and to make the people more aware of various cyber risks.

2.8. Summary

This chapter highlighted the position of Oman in terms of adopting the Internet and new ICT channels to support e-Oman implementation. E-government in Oman has been viewed as a part of e-Oman. E-Oman is at the initial stages of adoption and promotion. E-privacy concerns in Oman are also at relatively low levels but growing along with the expansion of e-services adoption by the Omani people. The chapter also described the Internet privacy protection efforts by the Omani government and concluded by presenting some key ICT awareness initiatives that the Oman government is
implementing to promote its e-Oman mission. However it is believed that Oman should do more to make the Omani people more confident in the technology, while being aware of Internet privacy issues.

Chapter 3 reviews the literature related to the research questions posed in this thesis.
Chapter 3. Literature Review

3.1. Introduction

The aim of this thesis is to examine the impact of e-privacy concerns on the use of e-government services. This chapter reviews the existing literature on Internet privacy (e-privacy) concerns and considers to what degree this factor and other related factors influence the intention to use online services. The main findings and views are presented to provide the required theoretical background for this study.

The chapter is divided into five main sections. After this introductory section, Section 3.2 provides background about e-service adoption and issues relating to e-privacy that might influence it. Section 3.3 discusses behavioural models of ICT usage and identifies the key factors influencing system usage. Section 3.4 reviews the literature relating to the main factors impacting on the acceptance of e-commerce and Section 3.5 discusses the major factors influencing the use of e-government services.

3.2. E-services adoption and use background

As defined by Sahai and Machiraju (2001), an e-service is a service provided via the Internet that assists users to complete tasks or conduct transactions. Therefore, e-services are typical services that are provided via the Internet for more efficiency. E-services encompass numerous sectors of social and public life, including information retrieval, e-commerce, e-learning, financial services, and e-government. Featherman and Pavlou (2003) state that e-services are a means of driving new revenue streams and creating efficiencies.
Nowadays, the use of the Internet as a medium for providing various services has expanded greatly. However, only focusing on the technology side of implementing e-services projects will not make e-services usage successful; users’ intentions to use information systems and the factors that influence their intentions have been found to be critical factors in achieving system success (Hartwick & Barki, 1994; Sahai & Machiraju, 2001). Various issues related to e-privacy which can impact on the adoption of e-services have been identified. The sections below provide background on them.

3.2.1. **E-privacy risk concerns**

Pfaffenberger describes privacy to be a basic necessity of liberty. He defines it to be the state of being left alone with no interruption or unnecessary monitoring while living or working, and as the right to have personal information not disclosed to the public without permission (Pfaffenberger, 1997). Canavan (2001) describes privacy as equivalent to ‘confidentiality’ or secrecy which refers to the protection of someone’s personal information from ‘unauthorized disclosure’. Camp (2000) describes privacy as “the right to be alone” (p. 115). Kizza (2002) defines privacy as consisting of some major rights. These rights include:

- The right to have ‘anonymity’;
- The safeguard of personal identity from public disclosure;
- Control and ownership of personal identity and information;
- Not to be under surveillance and unnecessarily monitored.

Graeff and Harmon (2002) note that data such as purchasing behaviour (favourite goods, loyalty discounts, bank and credit details), communication practices (phone, emails), daily movements (including traffic records), address details (work, residential), and personal identity information (name, gender, family etc.) is usually private.
Dinev, Bellotto, Hart, and Russo (2006) examined differences in individuals’ privacy concerns and beliefs about government surveillance in Italy and the United States. They found that users’ decisions to conduct e-commerce transactions on the Internet are influenced by privacy concerns. However, they found that Italians have lower levels of Internet privacy concerns than users in the U.S. Milne and Culnan (2004) claim that online users read online privacy policies because of their concern for privacy. They found that positive perceptions about notice comprehension increase trust in the notice. Therefore, they suggest that effective privacy notices serve an important function in addressing online risk issues which in return minimize risks of disclosing online personal information.

Many researchers have found that some organizations do not protect e-privacy (Brunk, 2002; Dinev & Hart, 2006b; Nath, 2005). Dhillon (2002) notes that the American Federal Trade Commission alone has conducted three studies between 1998 and 2000. These studies found that most Web sites were not practicing fair information practices. Other evidence of the growing concern about e-privacy is provided by the European Union Data Protection Directive which has been issued to protect European citizens from privacy attacks. The Directive’s articles prevent the transfer of individual information to places where local privacy laws are not compliant with the Directive. Both Salehnia (2002), and Dhillon (2002) identify the following four Internet privacy issues:

- Unfair collection;
- Massive collection of data in a huge number of databases across the globe;
- A growing amount of unauthorized access to data for secondary reasons;
- Higher chance of error occurrence.
Consumers are more protective of their personal data than most e-marketers probably ever expected. Indeed, any willingness by consumers to provide certain information online greatly depends on who is asking for it. Consumers are more willing to provide their home address, phone number, email address, Social Security number, and credit card number to a well-known site compared to a lesser-known site, in part because they have no confidence the e-commerce legal environment is secure (Nath, 2005).

Yu (2005) states that implementation of e-government cannot be separated from the collection and use of citizens’ personal information. Due to the potential serious influences of such issues on the adoption of e-services, many scholars have examined the impact of e-privacy concerns on the use of e-services and this research is described in Section 3.4 (e-commerce research) and Section 3.5 (e-government research).

3.2.2. **E-privacy protection**

The issues of privacy and security have been labelled by government and consumer organizations as two major concerns of e-commerce (Miyazaki & Fernandez, 2001). The importance of protecting Internet privacy, the different available solutions, and the issue of whose responsibility it is to protect Internet privacy must be considered.

Privacy protection is the process of securing the users’ online personal data. Suh and Han (2003) define e-privacy protection as the process of ensuring that personal information about customers collected from their online electronic transactions is secured from disclosure without permission. They believe that basic non-repudiation should include information confidentiality, privacy protection, and data integrity.
Suh and Han argue that five requirements are needed to achieve basic protection:

- Authentication to ensure that the trading parties in e-service transactions are who they claim to be;
- Non-repudiation so that trading parties do not deny their participation in an e-service transaction after the fact;
- Confidentiality to warrant that all communications between e-service transaction parties are restricted to the parties involved in the transaction;
- Privacy protection to ensure that online users’ personal information is protected from disclosure without permission;
- Data integrity such that data transmitted via the Internet is not created, intercepted, modified, or deleted illicitly.

Suh and Han (2003) and Schmid, Stanoevska-Slabeva, Tschammer (2001) believe that the basic requirements for e-privacy protection can be accomplished by using various technologies such as encryption, third-party certificates, digital signatures, and compliance with privacy policies. Other authors and studies have proposed some additional technological solutions such as: browsers and filters (Erbschloe & Vacca, 2001; Hahn, 2002), Self regulation and Platform for Privacy Preferences (P3P) (Chen & Rea, 2004), anonymity (Claessens, Diaz, Goemans, & Preneel, 2003), firewalls (Whitman & Mattord, 2005), and integrated mixed-technology solutions ("Dedicated security portfolio will blitz Internet threats", 2005).

Non-technical measures can also be applied to help increase e-privacy protection. These measures include increasing knowledge of online privacy issues awareness of Internet security and ways of protecting privacy (Cranor, 1998; Sheehan, 2004). Implementing e-transactions law is also a non technical way to enhance e-privacy
protection, and has been used by many countries across the world such as the United States, Australia, and most of the European countries (Connolly, 2004; Jackson, 2001; Park, Lee, & Ahn, 2004). According to Wildstrom ("Dedicated security portfolio will blitz Internet threats", 2005), the government as a legislative body should play a big role not only in setting up e-privacy law but also to enforce it in order to protect citizens from cyber threats. Consistent with this, many governments have established an independent body to oversee electronic transactions and information. For example, in December 2000 the Australian Federal government established the E-security Coordination Group (Jackson, 2001).

Other scholars have also argued that effective online policies are another non-technical solution that helps to protect e-privacy. Hahn (2002), Hunter (2002), Shalhoub (2006), Henderson, Snyder, and Byrd (2003), and many other scholars agree that websites that collect personal data should have online privacy policies that include an explanation of the following:

- The purpose of collecting the data;
- The location where data gets stored;
- Who can access the data;
- How the data can be corrected by the relevant individuals;
- Assurance statements that the data will be kept securely by the site;
- How individuals can “opt-out” when they need to.

Earp, Anton, Aiman-Smith, Stufflebeam (2005) argue that users should be aware of available online privacy policies and they should understand the content of these policies before starting to use services. They believe that awareness of e-privacy
protection can be increased through effective online polices and they think that website policies can guide customers browsing and transaction decisions.

3.2.3. **Trustworthiness of e-services**

Jarvenpaa and Tractinsky (1999) describe trust in the context of e-services as the belief or expectation that all the promises made by the service provider can be relied upon and that no one will take advantage of the consumer’s vulnerability. According to Serva, Benamati and Fuller (2005) and McKnight, Choudhury and Kacmar (2002), there is an important distinction between trust and trustworthiness. Generally trust is described as the willingness to depend on another in situations of risk, where trustworthiness usually refers to beliefs about the other party which precede that willingness to depend on one another. Heijden and Verhagen (2002) describe trustworthiness of a given service as the extent to which the online organization is perceived to be a reliable partner. Belanger, Hiller and Smith (2002) define trustworthiness as the users’ perceptions of confidence in the reliability and integrity of the e-service. This definition facilitates the examination of the nature of the relationships among trustworthiness, privacy, security, and the online users’ intentions to use e-services.

With the phenomenal growth of e-commerce and e-government services in recent years; scholars have increasingly investigated the significance of trust in information technology usage. Because of the global nature of the Internet as a public network, the issue of trust has even greater importance than in traditional services. Liu, Marchewka, Lu, and Yu (2005) found that privacy and trust remain potential obstacles to e-services adoption growth and important issues to both online individuals and organizations. Gefen, Karahanna, and Straub (2003) state that trustworthiness of a service can only exists if the consumer believes that the service provider has both the ability and the
motivation to deliver goods and services of the quality expected by the consumer. They also state that online trust is built through:

- A belief that the service provider has nothing to gain by cheating;
- A belief that there are safety mechanisms built into the Web site;
- By having a standard interface.

3.2.4. **E-privacy awareness**

The general definition of awareness provided by Ackerman and Mainwaring (2005) is knowing what others are doing or even that they are around. Scholars have defined awareness from a variety of perspectives. Solaru (2005) defined service awareness to be the extent to which an individual user is aware of the e-services application. Shaw, Chen, Harris, and Huang (2009) define security awareness as the degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels of information control to protect the stored data and networks.

It is widely believed that consumers’ awareness of e-privacy issues is lacking. Many scholars believe that there is limited awareness among online users of how much, and what information about consumers is stored in databases. They have also identified lack of knowledge about what service providers can do with information they have collected, and what regulations are available to protect consumers as aspects of the problem (Culnan & Armstrong, 1999; Dommeyer & Gross, 2003; Nath, 2005).
3.3. **Behavioural models relevant to information technology use**

This section reviews the main behavioural models of ICT usage in order to identify the key factors influencing system usage. Following the discussion of the main models of ICT usage, specific factors that may impact on the use of e-commerce and e-government services are considered in further detail.

### 3.3.1. *Main behavioural models*

Users and their perceptions are key factors in the success of newly introduced systems (Dinev et al., 2006; Hartwick & Barki, 1994; Suh & Han, 2003; Venkatesh, Morris, Davis, & Davis, 2003; Vijayasarathy, 2004; Warkentin et al., 2002). Researchers have attempted to explain the role of user perceptions in the adoption of new systems and technologies by using theories and models such as the Technology Acceptance Model (TAM) (Davis, 1989), Theory of Planned Behaviour (TPB) (Ajzen, 1991), Diffusion of Innovations Theory (Rogers, 1962) to explain the impact of different factors on users’ intentions to use information technology. These models have also been used to predict the intention to use e-services (e.g. Brown & Buys, 2005; Carter & Belanger, 2003; Featherman & Pavlou, 2003; Horst et al., 2007; Hsu & Chiu, 2004; Lee & Rao, 2005; Nath, 2005; Sahai & Machiraju, 2001; Wu & Chen, 2005).

TAM was introduced by Davis (1986) (see Figure 3.1). It was proposed to explain users’ intentions to use information technology solutions. The model proposes that perceived usefulness and ease of use jointly determine attitude toward using a system and this in turn influences actual level of use. Perceived usefulness was defined by Davis as "the degree to which a person believes that using a particular system would enhance his or her job performance" (Davis, 1989, p. 320). Ease of use is opposite to
complexity of use and it was defined by Davis as "the degree to which a person believes that using a particular system would be free of effort" (1989, p. 320). Davis (1993) tested the model and found that while both perceived usefulness and perceived ease of use played a role in predicting user attitudes toward using a system, the influence of perceived usefulness was 50% stronger than that of perceived ease of use.

Venkatesh and Davis (2000) provided a theoretical extension of TAM that explains perceived usefulness and usage intention in terms of social influence and other factors as shown in Figure 3.2. In addition to representing the impact of usefulness perceptions on usage intentions, TAM2 also suggests that social influence (subjective norm, voluntariness, and image) and cognitive instrumental processes (job relevance, output quality, result demonstrability, and perceived ease of use) significantly influence user acceptance and intention to use information technology.
Venkatesh, Morris, Davis, and Davis (2003) examined and tested eight prominent information technology acceptance models and based on this proposed their Unified Theory of Acceptance and Use of Technology (UTAUT). The eight models that were tested were TAM (Davis, 1989), the Motivational Model (Davis, Bagozzi, & Warshaw, 1992), the Theory of Reasoned Action (Ajzen & Fishbein, 1980), the TPB (Ajzen, 1991), a model combining TAM and TPB (Taylor & Todd, 1995b), the Model of PC Utilization (Thompson, Higgins, & Howell, 1991), Diffusion of Innovations Theory (Rogers, 1962), and Social Cognitive Theory (Bandura, 1986). As shown in Figure 3.3, the main constructs in UTAUT that are proposed to have a significant direct role in influencing behavioural intention to use a system are performance expectancy (perceived usefulness), effort expectancy (ease of use), social influence, and facilitating conditions. There are also four moderators of key relationships. These moderators are gender, age, experience and voluntariness of use. Venkatesh et al. (2003) argue that
proactively addressing the factors identified in UTAUT can help organizations to attract users to adopt and use new systems.

![UTAUT Model](image)

Figure 3.3 UTAUT (Venkatesh et al., 2003)

The theories and models presented above have been tested in many domains and many authors have adapted and extended them. The next section (Section 3.3.2) extends the discussion of key factors that have emerged from these models and that appear particularly relevant to the research described in this thesis. The following sections then look specifically at research that considers e-commerce (Section 3.4) and e-government adoption (Section 3.5).

### 3.3.2. **Key factors influencing system usage**

Perceived usefulness is widely supported as a key factor that influences behavioural intention as previously shown in TAM, TAM2, UTAUT, and many other models (Carter & Belanger, 2005; Davis, 1989; Fenech, 1998; Karahanna, Straub, & Chervany,

Social norms or subjective norms refer to users’ beliefs as to whether most other people who are important to them want them to perform a behaviour (note: this study uses the term social norms). These referents include people such as supervisors, subordinates, family members and peers. Social norms has been shown to be a significant predictor of behaviour (Bagozzi, 1992; Fishbein & Ajzen, 1975; Vijayasarathy, 2004) and social norms are believed to influence behavioural intention to use information systems via their affect on perceived usefulness (Davis et al., 1992; Kim, Kim, & Shin, 2009; Lee, Lee, & Lee, 2006; Ruth, 2000; Saha, 2008; Venkatesh & Davis, 2000).

The role of previous experience on the intention to use systems has been examined by many scholars. It has been found to play an important role in influencing users’ behaviour (Ajzen, 1991; Ajzen & Fishbein, 1980; Bagozzi, 1992; Fishbein & Ajzen, 1975; Taylor & Todd, 1995a). Ajzen and Fishbein (1980) believed that experience makes knowledge more accessible in memory. They argued that experience influences the users’ behavioural intention and that direct experience will result in a stronger, more stable behavioural intention. In TAM2, experience moderates the relationship between subjective norm and perceived usefulness which in turn impact the intention to use. The UTAUT model proposes that prior experience indirectly impacts intention to use via perceived usefulness and subjective norm (Venkatesh et al., 2003). Taylor and Todd (1995a) examined whether the determinants of information technology usage are the same for experienced and inexperienced users of a system and found significant differences in intention to use technology between experienced and inexperienced users.
3.4. Factors impacting e-commerce services usage

Henderson, Snyder, and Byrd (2003) define e-commerce as commercial transactions between organizations and customers to sell and buy goods and services using any type of ICT. E-commerce services are one form of e-service as mentioned at the beginning of Section 3.2. This section examines previous research in order to better understand the different factors that impact on e-commerce adoption by users. Although the research described in this thesis focuses on e-government services, much of the relevant literature relates to e-commerce. Therefore the research relating to factors that influence e-commerce service adoption will be reviewed first.

A number of studies have examined the factors that determine the adoption of e-commerce websites by users (e.g. Dinev & Hart, 2006b; Liu et al., 2005; Liu, Marchewka, & Ku, 2004; Nath, 2005; Park et al., 2004). Lee, Park, and Ahn (2001) built on TAM by incorporating the theoretical foundations of prior research in the theories of perceived risk (e.g. Bauer, 1960; Cox & Rich, 1964; Jarvenpaa, Tractinsky, & Vitale, 2000) to produce a new model called e-CAM to explain the adoption of e-commerce as shown in Figure 3.4.
In particular, Lee et al. (2001) examined the impact of perceived ease of use, perceived usefulness, perceived risk with products/services, and perceived risk in the context of the online transaction on the consumer’s purchasing behaviour. The antecedent constructs in the model were proposed to directly and/or indirectly affect consumers’ adoption of e-commerce services. Park, Lee, and Ahn (2004) validated the e-CAM in Korea and the USA. Their study supported the generalizability of e-CAM, and they suggested that e-service providers should consider these contextual factors in order to facilitate consumers’ adoption behaviour.

Several studies have specifically investigated the role of e-privacy concerns in adoption of e-services. Nath (2005) and Metzger (2004) studied consumers concerns about the availability of personal information on the Internet and their concerns relating to the possible abuse of personal information submitted online. Both studies found that e-privacy risk concern is a major factor that affects consumers’ adoption of online services. Nath’s (2005) study examined the influences on online information disclosure and found that online users’ concerns relate to unlawful information exchanges and their fears of violation of their individual privacy rights. Nath found that online users are not
confident that their e-privacy is protected and this causes an increase in their privacy concerns. Nath added that privacy concerns also increase through exposures in the media. Nath’s study concluded that privacy risk concerns negatively influence trust and online information disclosure. This study also investigated online information protection awareness and Nath suggests that consumers who are knowledgeable about privacy practices and options for securing their online information should take suitable actions to protect their e-privacy.

Online privacy concerns in the e-commerce domain have also been studied by Dinev and Hart (2006b), who examined the relationships between privacy concerns related to finding online personal information and privacy concerns related to the possible abuse of such information, and intended e-services use. They found that privacy concerns impact negatively on the information exchange. They also found that privacy concerns increase as the amount and sensitivity of personal information submitted through websites increases.

Belanger et al. (2002) investigated the factors impacting online users when purchasing online goods and services. They found that trustworthiness of websites services plays an important role and suggested that when online users make the decision to provide personal information online, they rely significantly on their perceptions of trustworthiness.

Liu, Marchewka, and Ku (2004) and Liu et al. (2005) also modelled the role of trust in the adoption of e-services. Their Privacy-Trust-Behavioural Intention Model as shown in Figure 3.5 suggests that there is a positive relationship between privacy and the degree of trust the consumer has in an e-commerce website, and that attempts to keep
data secure positively influence the customer’s level of trust. The model also indicates that trust in a corporate website influences intentions to use the site again, and whether users would recommend it to others (Liu et al., 2005; Liu et al., 2004). The model clearly suggests the importance of trust in consumers’ intentions to use and re-use e-services, and introduces the role of e-privacy protection by identifying security as part of privacy.

![Diagram](image)

**Figure 3.5 Privacy-Trust-Behavioral Intention Model (Liu et al., 2005; Liu et al., 2004)**

As shown in Figure 3.6, Kim, Kim, and Shin (2009) integrated social norms and electronic trust (eTrust) into their Airline B2C E-commerce Websites (AB2CEWS) acceptance model in order to determine their role in the acceptance of airline business-to-customer e-commerce websites. They hypothesized causal relationships between social norms and intention to reuse e-services, and between eTrust, and intention to reuse e-services. They found that both e-trust and social norms had a significant impact on users’ intentions to reuse e-services.
The importance of prior experience identified by Taylor and Todd (1995a) has been confirmed in the e-commerce domain by Suh and Han (2003) who found that users with higher levels of previous experience tend to accept more risk when using e-services. They also argued that previous experience is very important in creating and consolidating trust among e-services users.

Malhotra, Kim and Agarwal (2004) proposed and tested a model of the relationship between Internet users' information privacy concerns and intention to release personal information at the request of a marketer (see Figure 3.7). They found that the model explained a large amount of the variance in behavioural intention and concluded that the model provides a useful tool for analysing privacy threats on the Internet in terms of trusting beliefs, risk beliefs, and types of information.
Suh and Han (2003) investigated the impact of customer perceptions of security control on e-commerce acceptance. They found that perceptions of privacy protection and data integrity have indirect significant impacts on customers’ intentions to use e-commerce through their influence on trust. Gilbert, Balestrini, and Littleboy (2004) also examined the role of trust as well as the influence of financial security and information quality on e-services adoption. They found that these factors could be barriers to adoption when users are not assured that their financial data are secure, and that e-services grant them accurate and relevant information. They therefore stressed the importance of having e.privacy protected and controlled to support the adoption of e-services provided by Internet sites.

The research discussed above introduced perceived risk, privacy concerns, trust and previous experience as additional factors that play a role in the adoption of e-commerce services. The next section builds on this to look specifically at research in the e-government domain.
3.5. Factors impacting e-government services usage

Carter and Belanger (2005) define e-government services as the use of ICT to enable and improve the efficiency of the government services that are provided to citizens, employees, businesses, and agencies. According to Carter and Belanger, e-government services increase the convenience and accessibility of government services and information to citizens. Nowadays, government agencies around the world are increasingly making their services available online. E-government becomes especially important given its potential to reduce costs and improve service compared with traditional modes of government service delivery (Carter & Belanger, 2005; Lau, 2003). E-commerce and e-government both use the Internet as a medium to support the exchange of goods, information, and services between two or more parties. In e-government services the government allows the beneficiary to retrieve information and complete government transactions via the Internet. As with e-commerce, e-government has three e-services categories that are:

- Government to government (G2G) where the government provides various government departments with e-government services. This is comparable to business to business (B2B) in e-commerce;

- Government to business (G2B) where government provides businesses with e-government services. This is comparable to business to government (B2G) in e-commerce;

- Government to citizen (G2C) in which the government provides citizens with e-government services. This is comparable to business to customer (B2C) in e-commerce.

The success of both e-commerce and e-government services usage relies on the users’ willingness to adopt these services (Carter & Belanger, 2003; , 2005; Gefen et al., 2003;
Gefen & Straub, 2000; Pavlou, 2003). While e-commerce and e-government have a lot in common, there are differences. Carter and Belanger (2003) identify three main differences between them. The first difference is that where e-commerce can choose its customers, e-government services should be provided to the entire eligible population. The second difference is that the structure and decision making of businesses in the private sector is less centralized compared to government agencies. The third difference is accountability, where the government is obliged to allocate resources and provide the service in the best interests of the citizen.

In order to develop successful e-government services that provide participants with relevant information and quality services, government agencies must first understand the factors that influence citizen willingness to adopt this new form of services. Because of the similarity between e-government and e-commerce, researchers have used e-commerce adoption theories and models to study the adoption of e-government services. Consistent with the e-commerce research, researchers have found that perceived usefulness, social norms, previous experience, trust, e-privacy protection, and risk concerns are some of the factors that impact on users’ intentions to use e-government services (Belanger & Carter, 2008; Carter & Belanger, 2003; , 2005; Horst et al., 2007; Lee & Rao, 2005; Solaru, 2005; Srivastava & Teo, 2005). Models that specifically address e-government adoption are considered below, followed by a discussion of the research relating to each of the major factors believed to influence e-government adoption.

Warkentin et al. (2002) proposed an e-Government adoption model that includes many of the factors previously discussed (see Figure 3.8). They investigated online tax services in the USA and proposed that citizen trust is an important catalyst for
e-government adoption. They also proposed various ways to increase citizens’ trust and thus encourage the adoption of e-government services. Institution-based trust, such as an independent judicial system with appropriate legal powers, is the major tactic they proposed to build trust in e-government. They also suggested that the nature of previous interactions with the e-government system should be a major predictor of trust, and hence the intention to use an e-government service and continue to use it. Other factors shown to be influential in their research include perceived ease of use, perceived usefulness, perceived behavioural control, perceived risk and culture.

Figure 3.8 E-government Adoption Model (Warkentin et al., 2002)

Carter and Belanger (2003) used Moore and Benbasat’s (1991) perceived characteristics of innovating constructs to identify factors that influence citizen adoption of e-government initiatives. Their results agreed with Moore and Benbasat’s in that perceived relative advantage, perceived image, and perceived compatibility were found to be significant influences on e-government adoption.
In a later study, Carter and Belanger (2005) integrated constructs from TAM, Diffusion of Innovations Theory, and web trust models to examine the major factors influencing citizen adoption of e-government services (see Figure 3.9). Their study indicated that perceived ease of use, compatibility and trustworthiness are significant predictors of citizens' intentions to use an e-government service.

In 2008, Carter and Belanger further analysed the impact of trust and risk perceptions on citizens’ intentions to use e-government services, and explored the relationships between aspects of trust. They considered the roles of disposition to trust, trust of the Internet, trust of the government and perceived risk (see Figure 3.10). Their results showed that disposition to trust positively affects trust of the Internet and trust of the government, which in turn affect intentions to use an e-government service. Trust of the government also negatively influences perceived risk, which also affects intention to use (Belanger & Carter, 2008).
Kim (2008) extended TAM for the e-government domain by incorporating individuals’ privacy concerns and other variables. The study found that perceived risk plays an influential role in the citizens’ intentions to use e-government services and that citizens are more willing to use transactional e-government services when their online privacy concerns are addressed. He also found that when citizens perceive less risk their degree of trust toward e-government web sites and the government itself increase.

The models described above incorporate a number of factors relevant to the adoption of e-government services. The next sections extend the discussion of the factors that have emerged from these models and that appear particularly relevant to the research described in this thesis.

### 3.5.1. Previous experience

Tolbert and Mossberger (2003) studied whether e-government services increase the perceived trustworthiness of government or not. They were interested in exploring the potential for e-government to influence the citizens’ attitudes about government. They suggested that confidence in government increases based on actual prior experience with e-government and argued that experience contributes to citizens’ further use of
e-government services. Warkentin et al. (2002) also found that prior experience had a significant influence on the level of trust in e-government services.

3.5.2. **Perceived risks**

The role of perceived risks of using e-government services has been examined by various authors (e.g. Horst et al., 2007; Kim, 2008; Lee & Rao, 2005). Horst et al., (2007) undertook a study which aimed to identify the roles of risk perception and trust in the intention to adopt government e-services. They noted that citizens normally decide whether to adopt new e-government services by weighing up the benefits and risks. They found that risk perception was a significant factor influencing perceived usefulness of e-government services. The study specifically noted that e-privacy concerns are one of the main types of these perceived risks. Their findings are in agreement with those of Lee (2003) and Kim (2008) in regards to the role of perceived risks in the use of e-government services.

3.5.3. **E-privacy protection**

Yu (2005) conducted a study to examine the role of protection of citizens’ online information on the adoption on e-government services. Yu suggested that online information protection not only increases e-government usage but it helps in making such services more legitimate. These findings are consistent with those of Jho (2005) who argued that online protection should be enhanced in order to get citizens to use these services. Such protection could be done by having suitable laws, meaningful policy, and technology solutions. Hunter (2002) also suggests that preserving e-privacy protection will increase citizens’ involvement with and usage of e-government services. Stolfo, Johnson, Pavlicic, and Jan (2003) examined the influence of e-privacy protection on the intention to use and re-use e-government (as well as e-commerce) websites.
Their results suggest that citizens perceive e-government sites which use secure portals as much safer and are more likely to visit them again.

3.5.4. **Trust**

As indicated by the models, and research testing them, discussed above, trusting e-government services is essential to their adoption success. Srivastava and Teo (2005) also examined the role of citizen’s trust; their research concerned Singaporean e-government services adoption. They identified two dimensions of citizen’s trust in e-government: trust in the government’s commitment to e-government and ability and motivation to implement it, and trust in the enabling technologies. They found that these factors are major contributors to e-government adoption and acceptance. Horst et al. (2007) also investigated the role of trust in e-government adoption. They found that trust in e-government was the main determinant of the perceived usefulness of e-government services.

3.6. **The role of culture in adoption of e-services**

Chapter 2 describes how Oman is implementing a national project of e-government services in a culture that differs from the West. Oman is an Arab country which is considered to be a developing country in the Middle East and it has its own cultures and values. While less discussed in the literature, culture is an additional factor that may impact on the adoption and use of e-services. This section introduces this notion and discusses the literature on the role of culture in the acceptance of e-services in the e-commerce and e-government domains.

Seyal, Awais, Shamail, Abbas, and Andleeb (2004) describe culture as having a coherent set of beliefs with a set of shared core values. Thatcher, Foster, and Zhu
(2006) define culture as the idea that a group of people will feel, think and react similarly in a given context. Kedia and Bhagat (1988, p. 559) stated,

“Cultural variations across nations and organizational culture-based differences between organizations that are involved in the transfer of various kinds of technologies are considered two major factors that influence the success of transfer.”

Based on their review of the early literature on technology transfer between countries, Kedia and Bhagat (1988) found that social culture and organizational cultures are extremely important factors to be considered when transferring technology across cultures and from advanced countries to less advanced countries.

Although many studies have indicated that cultural factors do impact on e-services acceptance, there are some that have not identified effects. Thatcher et al. (2006) investigated the interaction of B2B e-commerce adoption decision factors. Their study provided insights into the impact of Chinese culture on B2B adoption and indentified that cultural factors do influence B2B e-commerce adoption decisions. Hoy and Lwin (2008) also found that organizational, industrial, governmental, and cultural factors do indeed influence B2B e-commerce adoption decisions. In addition, the nature of the cultural influence is dictated by industry conditions.

Sagi, Carayannis, Dasgupta, and Thomas (2004) stated that although many researchers argue that ICT is causing a globalized society, others consider that national culture is very important factor in the success of information technology projects. Their study examined this factor’s impact in the e-commerce domain by comparing the opinions of business students from the U.S., Greece and England about national control, privacy
cost, property rights and consumer preferences. They concluded that national culture significantly impacts attitudes towards e-commerce among cultural groups, and hence plays an important role in the use and acceptance of new technology.

In contrast to the studies described above, Liu et al. (2004) found no significant differences between Americans and Taiwanese in regards to privacy and trust concerns when purchasing online. Also, Jarvenpaa and Tractinsky (1999) found no significant cultural differences in the antecedents of trust of e-services, they did however suggest that further research was required.

Less research has been done on cultural influences on the adoption of e-government. In an early study, Warkentin et al. (2002) found that cultural factors such as uncertainty avoidance and power distance do impact the intention to engage in e-government. A recent paper by Shin, Song, and Kang (2008) argue that recent e-government projects in developing countries have made it possible to analyse e-government implementation and identify success and failure factors and stress that cultural aspects should be addressed during such analysis. Their study examined a set of factors that may impact on the success and the failure of e-government services projects. These factors included culture and values. Their findings support the claim that culture and values are major determinants of the successful implementation of e-government services projects in developing countries. Zhang, Guo, Chen, and Chau (2009) also demonstrated that cultural factors significantly impact end users' e-government services adoption and use.

The findings discussed above, both in the e-commerce domain, and e-government domain, suggest that e-service projects should adopt approaches that are culturally specific and tailored towards each culture’s perceptions.
3.7. Summary

The chapter examined and reviewed the literature related to the research questions posed in this thesis. Information technology adoption models and theories were discussed in relation to the adoption and use of e-services in both private and public organizations. E-privacy was found to be a factor that has been identified in a number of studies as impacting on the adoption of e-services. Many scholars encourage organizations to protect e-privacy as a way to increase e-service trustworthiness and therefore increase the intention to use both e-commerce and e-government services. The review of the literature also found that increases in e-privacy awareness lead to increases in e-privacy concerns, and that a number of authors have argued that it is necessary to increase users’ e-privacy protection readiness.

Chapter 4 follows on from this review of the literature and presents the research model proposed to answer the research questions for the thesis.
Chapter 4. Research Model

4.1. Introduction

This chapter presents the research questions for this thesis and introduces the proposed research model and associated hypotheses. The chapter is divided into four main sections. The research questions are presented in Section 4.2 and Section 4.3 defines each of the major constructs of interest. These definitions of the constructs are based on the literature review in Chapter 3. Section 4.4 presents the proposed research model and explains how it was developed. Section 4.4 also introduces and provides the justification for each of the hypotheses associated with the model.

4.2. Research objectives and questions

The research described in this thesis aims to examine the impact of online privacy concerns on citizens’ acceptance of e-government services (G2C). It also considers the role of information security and users’ ability to trust e-government services, given their privacy concerns. In order to address the research objectives, two high level research questions were proposed. These questions are as follows:

Q1. Do e-privacy risk concerns influence citizens’ intentions to use e-government services in Oman?

Q2. What other factors related to e-privacy influence citizens’ intentions to use e-government services in Oman?

Based on the literature review in Chapter 3, a number of factors that might play a role in influencing citizens’ intentions to use e-government services were identified. Section 4.3 provides definitions of these key constructs of interest. The literature review also
highlighted relationships and models relevant to this research on e-government adoption and Section 4.4 introduces the model that was proposed based on these.

4.3. **Constructs of interest**

This research assumes that the success of Oman’s e-government services project will be influenced by the citizens’ e-privacy risk concerns. As comprehensively discussed in Chapter 2 and Chapter 3, such concerns might preclude a large number of Omani citizens from using e-government services effectively. Similar problems have occurred in many commercial and governmental projects elsewhere across the world caused by many factors as discussed in Chapter 3 (Davis, 1989; Lee & Rao, 2005; Liu et al., 2005; Malhotra et al., 2004; Metzger, 2004; Olivero & Lunt, 2004; Taylor & Todd, 1995a; Venkatesh & Davis, 2000; Venkatesh et al., 2003). Therefore the research described in this thesis examines further the set of factors believed most likely to impact on citizens’ intentions to use e-government services in Oman: perceived usefulness, social norms, prior e-services experience, e-privacy risk concerns, e-privacy awareness, perceived e-privacy protection, perceived trustworthiness of e-government services. Most of these factors have not yet been studied adequately in the context of e-government adoption in Oman. The sections below provide definitions of each of the factors that are relevant to the context of this study.

4.3.1. **Perceived usefulness of e-government services**

Davis defined perceived usefulness as "the degree to which a person believes that using a particular system would enhance his or her job performance" (Davis, 1989 p. 320). Venkatesh et al. (2003) described perceived usefulness as the expected level that users believe they will get by using a particular system. Consistent with previous literature this study defines perceived usefulness of e-government services as the degree to which
a citizen believes that using e-government services would enhance his or her ability to obtain information and conduct transactions with the government.

4.3.2. **Social norms**

Social norms refer to users’ beliefs as to whether or not their significant others want them to perform a behavior. In the domain of e-services, influences could be from family members, friends, co-workers and even supervisors at work (Hsu & Chiu, 2004). Social norms are defined in the context of this study as the beliefs of the citizen as to whether or not significant others want them to use e-government services. The people might include family members, friends, co-workers and supervisors at work.

4.3.3. **Prior e-services experience**

Jarvenpaa et al. (2000) note that prior experience with online services leads to more knowledge and better understanding of consequences that can influence beliefs and attitudes related to future use. Prior experience is normally defined in terms of how often a user uses the service and/or how much they know about e-services. For example, Horst et al. (2007) define e-service prior experience as the number of times a user has used a specific e-service and the number of different e-services a user has used, and Wakentin et al. (2002) view prior e-services experience as the previous familiarity and interaction with e-service sites. This study defines prior e-services experience as the amount of previous hands on experience with e-services that a citizen has had.

4.3.4. **E-privacy risk concerns**

E-privacy has been identified as a key factor of concern among online users and many authors believe that it might become one of the most important barriers to e-services development (Dinev & Hart, 2006b). Therefore, e-privacy risk concerns are a potential
obstacle to e-services growth and an important issue to both individuals and government organizations. Dinev and Hart (2006a) defined e-privacy concerns in terms of two main dimensions; these are concerns related to unauthorized access or interception of the users’ personal information and concerns related to the possible misuse and damaging of such information. E-privacy risk concerns, as described by Pavlou (2003), are potential worries of losing control over the personal information, such as when someone uses the personal information of somebody else without the latter’s knowledge and permission.

This study defines e-privacy risks concerns as the citizens’ concerns regarding potential loss of control over personal information, such as when information about a citizen, obtained during their use of e-government services, is used without permission.

4.3.5. **E-privacy awareness**

Security awareness was defined by Shaw et al. (2009) as the degree of understanding users have about the importance of information security and their role in it. Olivero and Lunt (2004) define risk awareness as the amount a person knows about online risks that are associated with a given service. This could include knowledge about personal information threats, such as errors, unauthorised use, breaches of privacy, ways of protecting online personal information, and government measures of e-privacy protection.

For the study described in this thesis, e-privacy awareness is defined as the amount citizens know about online e-privacy risks, and about related issues such as how to protect themselves and what protection is provided by the service provider.
4.3.6. **Perceived e-privacy protection**

E-privacy protection is the protection of customers’ online personal information from any type of unauthorized electronic transaction or disclosure without permission (Suh & Han, 2003). Liu et al. (2005) define perceived e-privacy protection as the degree to which users believe that facilitating conditions exist that can protect their online information from disclosure and use without permission.

In this study, perceived e-privacy protection is defined as the degree to which a citizen believes that facilitating conditions (technical and organizational) exist that can protect his/her online privacy while using e-government services.

4.3.7. **Perceived trustworthiness of e-government services**

Jarvenpaa et al. (2000) define trust as the governing mechanism in a given exchange relationship that is characterized by uncertainty, vulnerability, and dependence. Specifically, it is the confidence that an online consumer has to use e-services. Such confidence is based on the consumer’s beliefs that the e-services can be relied upon to protect her/his online privacy (Jarvenpaa et al., 2000). Heijden and Verhagen (2002) describe the trustworthiness of a given service as the extent to which the online organization is perceived to be reliable, and Belanger et al. (2002) define trustworthiness as the users’ perceptions of confidence in the reliability and integrity of the e-service. Thus, trustworthiness refers to the users’ beliefs and expectations about the service provider’s ability and motivation to deliver reliable goods and services. This study defines perceived trustworthiness of e-government services as the citizen’s perceptions of the integrity of e-government services and the extent to which they can be trusted.
4.3.8. **Intention to use e-government services**

As viewed by Ajzen (1985), behavioural intention is an indication of an individual's readiness to perform a given behaviour. Suh and Han (2003) define behavioural intention as the level of strength of a user’s intention to do a particular behaviour. It is assumed to be the immediate antecedent of the behaviour and has frequently been used as an indicator of users’ acceptance and adoption of new systems (Carter & Belanger, 2005; Suh & Han, 2003; Venkatesh & Davis, 2000).

Based on previous definitions, this study defined the intention to use e-government services as the individual’s willingness to use e-government services sites.

Table 4.1 provides a summary of the research constructs of interest and their associated definitions based on the discussion above.
<table>
<thead>
<tr>
<th>Construct</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-privacy risk concerns</td>
<td>E-privacy risk concerns are citizens’ concerns regarding potential loss of control over personal information, such as when information about a citizen, obtained during their use of e-government services, is used without permission.</td>
</tr>
<tr>
<td>Perceived e-privacy protection</td>
<td>Perceived e-privacy protection is the degree to which a citizen believes that facilitating conditions (technical and organizational) exist that can protect his/her online privacy while using e-government services.</td>
</tr>
<tr>
<td>Social norms</td>
<td>Social norms are the beliefs as to whether people who are important to citizens want them to perform a particular behavior or not. In this case, the behavior is use of e-government services, and the other people might include family members, friends, co-workers and supervisors at work.</td>
</tr>
<tr>
<td>Perceived usefulness of e-government services</td>
<td>Perceived usefulness of e-government services is the degree to which a citizen believes that using e-government services would enhance his or her ability to obtain information and conduct transactions with the government.</td>
</tr>
<tr>
<td>Perceived trustworthiness of e-government services</td>
<td>Perceived trustworthiness of e-government services relates to the citizen’s perceptions of the integrity of e-government services and the extent to which they can be trusted.</td>
</tr>
<tr>
<td>Intention to use e-government services</td>
<td>Intention to use e-government services relates to an individual’s willingness to use e-government services sites.</td>
</tr>
<tr>
<td>E-privacy awareness</td>
<td>E-privacy awareness is the amount a citizen knows about online e-privacy risks, and about related issues such as how to protect his or her self, and what protection is provided by the service provider.</td>
</tr>
<tr>
<td>Prior e-services experience</td>
<td>Prior e-services experience is the amount of previous hands on experience with e-services that a citizen has had.</td>
</tr>
</tbody>
</table>

### 4.4. The research model and hypotheses

A model was proposed to provide a framework for this research and to define the research boundary (see Figure 4.1). The model has a firm base in the literature and is
intended to provide a better understanding of the inter-relationships that exist between the different factors identified as likely to play a role in e-government acceptance. The model uses Liu et al.’s (2005) privacy-trust-behavioural intention model and Malhotra’s et al. (2004) model as a starting point. Both models provide frameworks to explain the role of e-privacy concerns in relation to the adoption success of e-services. Both models emphasise the relationship between e-privacy risk concerns and the level of trust, and the relationship between level of trust and intention to use e-government services. These relationships provide the initial basis for the proposed model.

The broader technology acceptance literature and recent work on e-privacy awareness and protection were used to identify additional factors likely to influence e-government acceptance and to identify the way in which these factors might act. Warkentin et al.’s (2002) e-government adoption model proposes a relationship between prior e-services experience and level of trust, and Suh and Han’s (2003) research model links perceived e-privacy protection and level of trust. These relationships were incorporated into the proposed model.

Carter and Belanger’s (2005) and Lee and Rao’s (2005) models suggest the relationships between perceived usefulness of e-services and intention to use these services, and between perceived trustworthiness of e-services and the intention to use these services. Horst et al. (2007) found that trust in e-government was an important determinant of the perceived usefulness of e-government services. These relationships were also all included in the proposed model.
Venkatesh and Davis (2000) included social norms as an influence on perceived usefulness in TAM2. Not many studies have addressed the relationship between social norms and perceived trustworthiness of e-services. Kim et al. (2009) and Li, Hess and Valacich (2006) are among the very few who have examined the relationship but their work was in the e-commerce environment. Both studies found that social norms significantly impact the level of trust of e-commerce services. Therefore, the relationship was included in the proposed model.

Lee et al. (2001) specifically address the relationship between perceived risks with e-services and perceived usefulness in their e-CAM model, and this relationship was considered important for the study described in this thesis. The relationship was therefore included in the model.

The proposed model has 11 associated hypotheses. Each of the hypothesized relationships is presented and justified below.
Many authors have investigated the direct impact of social norms on behavioral intention (Bhattacherjee, 2000; Karahanna et al., 1999; Venkatesh et al., 2003) however fewer have studied the relationship between social norms and perceived usefulness. Venkatesh and Davis (2000) and Schepers and Wetzels (2007) are among those who have studied this relationship and both studies found that social norms significantly influence perceived usefulness, but their studies were not in the e-government environment. Horst et al. (2007) and Jaeger and Thompson (2004) have studied the relationship in the e-government domain and found that social norms significantly impact the perceived usefulness of e-government services and indirectly impact intention to use e-government services.

In the context of this study, Oman has a small society and many people know each other and have strong inter-relationships, especially at work. They tend to talk over things that are newly introduced to the society, and thus have many opportunities to influence one another about the benefits of the e-government services project. Therefore, and consistent with literature it was proposed that:

**Hypothesis H1:** Social norms will positively influence the level of perceived usefulness of e-government services.

As previously discussed, the influence of social norms on perceived trustworthiness of e-government services was not been previously studied. In both the e-commerce and e-government domains, Bolton, Katok, and Ockenfels (2004) and Horst et al. (2007) have argued that social norms is an important factor impacting the level of trustworthiness of e-services, but have not tested the relationship. Li et al. (2006) have examined the relationship and found that social norms significantly impact the level of
trust in e-commerce services. Consistent with this the following hypothesis was proposed:

**Hypothesis H2:** Social norms will positively influence the level of perceived trustworthiness of e-government services.

Prior experience has been shown to be a factor influencing behavior in many previous studies as discussed in Chapter 3. A study by Horst et al. (2007) tested an indirect relationship between previous experience and trust in e-government services. They found that the more previous experience users have, the less risk they perceive, and the more they trust in government e-services. Warkentin et al. (2002) also found that previous interactions with e-government services are a major predictor of trust of these services and they suggested that culture may play a role in the relationship. At this stage Omanis do not have much experience with e-services, however consistent with previous research it is expected that the more experience they have, the more trust they will have in e-government services, therefore the following hypothesis was proposed:

**Hypothesis H3:** Prior e-services experience will positively influence the level of perceived trustworthiness of e-government services.

Consciously and unconsciously citizens perceive risk when evaluating the use of e-government services (Featherman & Pavlou, 2003; Gilbert et al., 2004; Horst et al., 2007; Yu, 2005). Featherman and Pavlou (2003), in the e-commerce domain, found that the more risks of using e-services that users perceive, the less useful they believe the e-services are. Horst et al. (2007) identified a negative impact of e-privacy concerns on both the perceived usefulness of generic e-services and e-government services in one of two groups examined, but not in the other. This indicates that further research is required to understand this relationship. For this study, it was proposed that higher
levels of e-privacy risk concerns will be significantly associated with decreases in the perceived usefulness of e-government services:

**Hypothesis H4:** E-privacy risk concerns will negatively influence the perceived usefulness of e-government services.

It has also been found that e-privacy risk concerns play an essential role in influencing the level of trustworthiness of a specific e-service, such that the higher the perceived risk is, the lower the levels of trust are (Horst et al., 2007; Liu et al., 2005; Liu et al., 2004; Metzger, 2004; Reilly & Cullen, 2007; Suh & Han, 2003). Because such concerns can influence the level of trust in e-government services, e-privacy risk concerns are considered to be a possible risk factor for the e-government services project in Oman. Hence it was hypothesized that:

**Hypothesis H5:** E-privacy risk concerns will negatively influence the level of perceived trustworthiness of e-government services.

Many scholars believe that although e-privacy security measures have advanced, users still do not fully trust e-services and are looking forward to having better protection measures (Carter & Belanger, 2005; Jho, 2005; Lau, 2003; Lee & Rao, 2005; McDonagh, 2002; Srivastava & Teo, 2005; Warkentin et al., 2002; Yu, 2005). Studies by Lee et al. (2001) and Loukides and Shao (2007) in the e-commerce domain both found that risk protection significantly influences the perceived usefulness of e-services. Horst et al. (2007) studied the relationship in the e-government domain but only identified a significant relationship between risk protection and perceived usefulness in one of two samples they used. However given the support in the e-commerce domain it was hypothesized that:
**Hypothesis H6:** Perceived e-privacy protection will positively influence the level of perceived usefulness of e-government services.

For many years, the impact of perceived e-privacy protection on the intention to use e-services has been studied from the e-commerce perspective and studies have found that perceived e-privacy protection has a significant impact on trust in e-commerce (Metzger & Docter, 2003; Nath, 2005; Suh & Han, 2003), but fewer studies have considered the e-government perspective. Among those who have studied the subject from an e-government perspective are Lee et al. (2003) and Jho (2005). They found that security issues and concerns appear when security measures are weak or absent. They also found that the more that users perceive protection is in place for the e-service, the more trust is created. As Oman doesn’t yet have good levels of e-services protection it is important to examine the impact of protection measures on the level of perceived trustworthiness. Consistent with the previous literature it was hypothesized that:

**Hypothesis H7:** Perceived e-privacy protection will positively influence the level of perceived trustworthiness of e-government services.

E-privacy awareness relates to how much citizens know about online e-privacy risks and about related issues such as how to protect themselves and what protection is provided by the service provider. Previous studies such as Dinev and Hart (2006), Olivero and Lunt (2004), Schmid et al. (2001), and Malhotra et al. (2004) have all indicated that e-privacy awareness increases concerns about e-privacy risks. These studies were in the e-commerce domain. Solaru (2005) is among the very few authors who have studied the impact of awareness in relation to e-government services, Solaru found that awareness is the first step of the adoption process, and forms the basis for any further evaluation decision. However Solaru examined service awareness
(awareness of service availability and quality) and not e-privacy awareness as is defined in this study. Because previous studies have found that awareness can play a critical role in this study hypothesized that:

**Hypothesis H8:** E-privacy awareness will positively influence the level of e-privacy risk concerns.

Research on the relationship between perceived trustworthiness and perceived usefulness of e-government services has indicated that unless e-government services are seen as trustworthy, their perceived usefulness is very limited (Horst et al., 2007; Lee & Rao, 2005; Liu et al., 2005; Reilly & Cullen, 2007). Consistent with this previous research it was therefore hypothesized that:

**Hypothesis H9:** Perceived trustworthiness of e-government services will positively influence the level of perceived usefulness.

As discussed in Chapter 3, many researchers have suggested that lack of perceived trustworthiness of online partners (in relation to handling and storage of online personal information) has excluded a substantial number of users from enjoying the benefits of e-services. Confidence in the available e-services is a significant factor in determining use of these services (Belanger et al., 2002; Liu et al., 2005; Malhotra et al., 2004). Consistent with the existing literature this study proposes that trustworthiness of e-government services will significantly impact on the intention to use e-government services in Oman, hence it was hypothesized that:

**Hypothesis H10:** Perceived trustworthiness of e-government services will positively influence the intention to use e-government services.
Perceived usefulness has been shown to be a significant factor influencing the decisions of users to use information systems and e-services (Pavlou, 2003; Venkatesh et al., 2003; Warkentin et al., 2002). There is also some evidence of its role with respect to e-government services (Carter & Belanger, 2005; Lee et al., 2003; Lee & Rao, 2005).

Therefore consistent with this research it was hypothesized that:

**Hypothesis H11**: Perceived usefulness of e-government services will positively influence the intention to use e-government services.

Table 4-2 Summary of the research hypotheses

<table>
<thead>
<tr>
<th>Hypothesis</th>
<th>Description of hypothesis</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1</td>
<td>Social norms will positively influence the level of perceived usefulness of e-government services.</td>
</tr>
<tr>
<td>H2</td>
<td>Social norms will positively influence the level of perceived trustworthiness of e-government services.</td>
</tr>
<tr>
<td>H3</td>
<td>Prior e-services experience will positively influence the level of perceived trustworthiness of e-government services.</td>
</tr>
<tr>
<td>H4</td>
<td>E-privacy risk concerns will negatively influence the level of perceived usefulness of e-government services.</td>
</tr>
<tr>
<td>H5</td>
<td>E-privacy risk concerns will negatively influence the level of perceived trustworthiness of e-government services.</td>
</tr>
<tr>
<td>H6</td>
<td>Perceived e-privacy protection will positively influence the level of perceived usefulness of e-government services.</td>
</tr>
<tr>
<td>H7</td>
<td>Perceived e-privacy protection will positively influence level of perceived trustworthiness of e-government services.</td>
</tr>
<tr>
<td>H8</td>
<td>E-privacy awareness will positively influence the level of e-privacy risk concerns.</td>
</tr>
<tr>
<td>H9</td>
<td>Perceived trustworthiness of e-government services will positively influence the level of perceived usefulness of e-government services.</td>
</tr>
<tr>
<td>H10</td>
<td>Perceived trustworthiness of e-government services will positively influence the intention to use e-government services.</td>
</tr>
<tr>
<td>H11</td>
<td>Perceived usefulness of e-government services will positively influence the intention to use e-government services.</td>
</tr>
</tbody>
</table>
4.5. **Summary**

This chapter introduced the research model and its major components. In the first section the research objectives and main questions were highlighted. The second section defines the main constructs for this study. Seven constructs were defined and presented as the factors most expected to influence directly and indirectly the intention to use e-government services in Oman. These factors are e-privacy risk concerns, perceived e-privacy protection, social norms, prior e-services experience, e-privacy awareness, perceived trustworthiness of e-government services, and perceived usefulness of e-government services. The proposed model was then presented and its derivation explained. The last part of the chapter introduced and provided the justification for the hypotheses associated with the model. The next chapter discusses the research methodology and data analysis techniques.
Chapter 5. Research Methodology

5.1. Introduction

This chapter discusses the research methodology that was used for the study. This methodology included both quantitative and qualitative approaches. Section 5.2 discusses triangulation and its importance in strengthening the research findings. The study’s participants are described in Section 5.3. Section 5.4 discusses the questionnaire design and development and also discusses the pre-testing of the questionnaire and pilot study. Section 5.5 discusses the data collection procedures associated with the questionnaire and Section 5.6 describes the procedures associated with the data collection via interviews. Section 5.7 provides an overview of the data analysis procedures and techniques for both the quantitative and the qualitative parts of the study.

5.2. Triangulation of Method

Triangulation of methods mixes quantitative and qualitative data collection approaches to maximize the strength of the collected data (Maanen, 1983). Triangulating data collection is recommended to increase the validity and reliability of research findings based on the assumption that multiple approaches most likely produce different results to be compared and matched (Neuman, 2003; Oates, 2006) and thus explain more fully the richness and complexity of the behaviour being considered. The most common triangulation types are triangulation of measures, triangulation of observers, triangulation of theory, and triangulation of method (Merriam, 1988; Oates, 2006).

This research used triangulation of method, using the two most well known techniques for data collection: using a questionnaire on a fairly large number of citizens, and some
focused semi-structured interviews. The interviews were intended to complement the questionnaire findings by collecting in-depth details of the impact of e-privacy risk concerns among citizens on their intentions to use e-government services. In this sense both quantitative and qualitative approaches were used in a complementary manner.

5.3. Participants

The target population for this study was Omani citizens. The sampling frame was civil services government employees in Oman. However, the focus was on them as citizens, not as employees, and they were asked to express their views as citizens not as government employees. Confidentiality was granted to all participants in this research at all stages. Civil service employees comprise the largest national sector in terms of number of employees, with more than 110,000 employees (Ministry of Civil Service, 2007). More than 75% of them are Omanis. These employees vary in age and information technology background. About 45% of them are women and 55% men. Their social and cultural backgrounds are quite homogeneous (Ministry of Civil Service, 2007). According to the Omani national census of 2003, civil service employees form more than 93% of the total number of government employees. They also form about 20% of all Omani manpower (Ministry of National Economy, 2008).

The samples for the questionnaires and the interviews were selected from a wide range of government units within the civil service sector. They were chosen from different positions and ranks and vary in terms of age, gender, education levels, and Internet experience. However, both samples share common characteristics in that all participants were either Omani citizens or Omani residents who were potential candidates for the use of Omani e-government services in one way or another.
5.4. **Development of the questionnaire**

Surveying is known as a data collection approach that can generate precise findings and indications about large populations. Although there are other survey techniques such as secondary research, direct measurement, and observation, for a lot of people, survey by questionnaire and/or interviews is the first choice (Oates, 2006). Many prior researchers have used the questionnaire approach to study information technology adoption and use (e.g. Bedford, 2005; Gilbert et al., 2004; Horst et al., 2007; Liu et al., 2005; Suh & Han, 2003).

5.4.1. **Questionnaire design**

Peterson (2000, p. 12) states that “the quality of the information obtained from a questionnaire is directly proportional to the quality of the questionnaire”. The questionnaire for this study was carefully designed to consider the major design issues such as the length, order and sequence of questions, wording, and layout (Oppenheim, 1966; Rea & Parker, 2005). The initial proposed questionnaire for this study consisted of 83 questions and it was shortened to 56 questions based on the pilot test findings and feedback as discussed in Section 5.4.3. The English version was the source of the Arabic version. The questionnaire was translated to Arabic, and then cultural aspects were also addressed by using the recommended terms for questionnaires from the Omani Ministry of National Economy web site (www.mone.gov.om) and by consulting sample questionnaires from the site.

Appendix A provides the English version of the final Questionnaire and Appendix B provides the Arabic version of it. The Arabic version was used to collect the data (as the target population is Arabic speaking) while the English version remained for the documentation purposes of this study.
The questionnaire started with a covering letter introducing the research, and providing contact details for the researchers. A key words definition list was also placed at the beginning of the questionnaire to ease subject understanding and to minimize the chance of any possible ambiguity. A brief description of e-government service initiatives in Oman was also added to illustrate the existence of e-government services in Oman as many citizens might not have been aware of this. The questionnaire consisted of 7 parts (A – G) containing, as previously mentioned, 56 Items. To enhance the questionnaire flow, each part was preceded by a brief introduction. The structure of the final questionnaire and measurement of constructs is discussed below.

5.4.1.1.  Background information

The first part of the questionnaire (Part A) was used to collect basic demographic and background information about the participants. It consisted of 6 items as shown in Table 5.1. Age was measured on a three category scale (18-29; 30-49; 50+). Level of education was measured using four categories (High school or less; Some college; College graduate; Postgraduate). Level of experience using the Web and level of experience using e-government services were both measured on a four point scale (None; Beginner; Intermediate; Advanced). These items were collected to help in characterizing the participants based on their age, gender, and education and to establish a better understanding of the participants’ background experience and skills. This part was kept short and simple to encourage the participants to proceed to completion of the questionnaire.
Table 5-1 Background and demographic items

- How old are you?
- What gender are you?
- What level of education do you have?
- What is your World Wide Web experience level?
- What is your e-government services experience level?
- Have you taken any formal Internet training?

5.4.1.2. **Perceived usefulness**

Perceived usefulness was measured on a five point Likert scale labelled from ‘strongly disagree’ to ‘strongly agree’ (see Part B of questionnaire in Appendix A). The items used to measure this construct are listed in Table 5.2. Four items are from Davis (1989). Slight modifications to wording were made to suit the e-government domain. To further customize the measurement to better suit e-government services, two extra items were developed for this study.

Table 5-2 Perceived usefulness items

- The content of the e-government sites would be useful to me.
- E-government services would enhance my effectiveness in searching for government information
- Using e-government services would improve my government transaction performance.
- Using e-government services would increase my overall productivity.

*The two items developed for this study:*

- E-government sites would provide valuable services for me.
- Using e-government services would make it easier to interact with the government.
5.4.1.3. **Social norms**

The four items used to measure social norms are presented in Table 5.3 (see Part B of questionnaire in Appendix A). These items are from Hartwick and Barki (1994) and have been adapted by Hsu and Chiu (2004). No further modifications were made. They were measured on a five point Likert scale labelled from ‘strongly disagree’ to ‘strongly agree’.

Table 5-3  Items to measure social norms

- People I know think that using the e-government services is a good idea.
- My colleagues think I should use the e-government services.
- My friends think I should use the e-government services.
- My family think I should use the e-government services.

5.4.1.4. **Prior e-services experience**

The items used to measure prior e-services experience are shown in Table 5.4 (see Part C of questionnaire in Appendix A). The first two items were taken from an instrument used by Jarvenpaa et al. (2000) and were reworded slightly to suit government services usage. Three additional measurement items were developed for the study. All items were measured on a five point Likert scale labelled from ‘strongly disagree’ to ‘strongly agree’.
Table 5-4  Items to measure prior e-services experience

- I frequently use the Internet to find information about services and products.
- I frequently pay for products or services on the Internet using e-services sites.

*Items developed for this study*:  
- Many times I have requested further information about certain products or services on the Internet.
- I have disclosed my personal information to e-services sites several times.
- So far, I have conducted many e-services through the available websites.

5.4.1.5.  *E-privacy risk concerns*

Eight items from Smith, Milberg, and Burke (1996) were used to measure participants’ e-privacy risk concerns related to the use of e-government services (see Part D of questionnaire in Appendix A). As the original items were used to measure e-privacy concerns in the e-commerce field some items were found not to be suitable for the government environment. For example, government units are not expected to sell the collected information for money as the government is assumed to have governance objectives and purposes. Therefore only eight items were selected out of 15 items that were used by Smith et al.. Modifications were made to the selected items to suit the e-government domain. The items were measured on a five point Likert scale labelled from ‘strongly disagree’ to ‘strongly agree’ and are shown in Table 5.5.
Table 5-5 Items to measure e-privacy risk concerns

- I'm concerned that e-government sites will collect too much personal information about me.
- It would bother me if e-government sites asked for personal information.
- E-government sites should not use personal information for any purpose unless it has been authorized by individuals who provided the information.
- If e-government sites ask me for personal information, I would think twice before providing it.
- E-government sites should take more steps to make sure that the personal information in their files is accurate.
- E-government sites should have better procedures to correct errors in personal information.
- E-government sites should never share personal information with other government units unless it has been authorized by the individuals who provided the information.
- E-government sites should take more steps to make sure that unauthorized people cannot access personal information in their computers.

5.4.1.6. E-privacy awareness

E-privacy awareness was measured using four items. These items are listed in Table 5.6 (also see Part D of questionnaire in Appendix A). Two of these items were taken from an instrument developed by Olivero and Lunt (2004) and were reworded to suit use in an e-government environment. Two items were developed specifically for the study. E-privacy awareness was measured on a five point Likert scale labelled from ‘strongly disagree’ to ‘strongly agree’.
Table 5-6 Items to measure e-privacy awareness

- I am aware that my personal information could be transmitted to other government units.
- I am aware that whenever I give my personal information to any e-government site it could be accessed by many others.

*Items developed for this study:*
- I am aware of e-privacy risks.
- I am aware that my personal information given to e-government sites could be used to track my online behaviour.

5.4.1.7. *Perceived e-privacy protection*

Perceived e-privacy protection was measured using five items as shown in Table 5.7 (also see Part D of questionnaire in Appendix A). Perceived e-privacy protection was measured on a five point Likert scale labelled from ‘strongly disagree’ to ‘strongly agree’. The items were taken from an instrument used by Liu et al. (2005). Some wording was altered to suit the e-government environment.

Table 5-7 Items to measure perceived e-privacy protection

- E-government sites will devote time and effort to preventing unauthorized access to my personal information.
- I feel that e-government sites will not release personal information about me without my express permission.
- I feel that e-government sites would make a reasonable effort to ensure that the information collected about me is accurate.
- E-government sites would have a mechanism to review and change incorrect personal information.
- E-government sites would give me a clear choice before disclosing personal information about me to third parties.
5.4.1.8. *Perceived trustworthiness of e-government services*

Six items were used to measure perceived trustworthiness of e-government services as shown in Table 5.8 (see Part E of questionnaire in Appendix A). The first four items were taken from an instrument used by Carter and Bélanger (2005) in combination with one item from Suh and Han (2003). The item from Suh and Han was added to strengthen data collection. The items were slightly reworded to suit the e-government domain. Perceived trustworthiness of e-government services was measured on a five point Likert scale labelled from ‘strongly disagree’ to ‘strongly agree’.

Table 5-8  Items to measure perceived trustworthiness of e-government services

<table>
<thead>
<tr>
<th>Items from Carter and Belanger (2005)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The Internet has enough safeguards to make me feel comfortable using it</td>
</tr>
<tr>
<td>to interact with the government.</td>
</tr>
<tr>
<td>• In general, the Internet is now a robust and safe environment for</td>
</tr>
<tr>
<td>e-government services transactions.</td>
</tr>
<tr>
<td>• I think I trust Omani e-government services sites.</td>
</tr>
<tr>
<td>• I think Omani e-government sites will be trustworthy.</td>
</tr>
<tr>
<td>• E-privacy security policies and precautions of Omani e-government sites</td>
</tr>
<tr>
<td>will make me feel that the services are trustworthy.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Items from Suh and Han (2003)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Omani e-government sites will keep citizens’ best interests in mind.</td>
</tr>
</tbody>
</table>

5.4.1.9. *Intention to use e-government services*

Intention to use e-government services was measured using the five items shown in Table 5.9 (see Part F of questionnaire in Appendix A). Four of these items were taken from an instrument developed by Gefen and Straub (2000) and were also used by Carter and Belanger (2005). The fifth item was taken from an instrument by Suh and Han (2003). Item wording was modified slightly to suit use in the e-government domain.
Intention to use e-government services was measured on a five point Likert scale labelled from ‘strongly disagree’ to ‘strongly agree’.

Table 5-9  Items to measure intention to use e-government services

Items from Gefen and Straub (2000):
- I would use the e-government services to gather governmental information.
- I would use e-government services provided over the web.
- Interacting with the government over the web is something that I would do.
- I would be willing to provide personal information to e-government sites.

Items from Suh and Han (2003):
- I would be willing to recommend others to use and disclose their personal information to e-government sites to interact with government through the e-government sites.

5.4.1.10. **Actual use of e-government**

Although actual use was not part of the proposed model; it was measured in Part F of the questionnaire so that it could be descriptively examined to draw a clearer picture of e-government services use in Oman. Actual use was measured using seven items. These items were measured using several different scales as shown in Table 5.10 below and some modifications to some wording were made so that they were appropriate for the use of e-government services. Five items were from an instrument from Vijayasarathy (2004). The sixth item was used by Suh and Han (2003) in their instrument to study the use of e-commerce. A seventh item was added to further identify the nature of use in Oman.
Table 5-10  Items to measure actual use

*Items from Vijayasarathy (2004)*
- I have disclosed my personal information to e-government sites several times. (5 point scale from ‘Never’ to ‘Always’)
- I frequently pay for government services through e-government sites. (5 point Likert scale)
- On average each month, how many hours do you spend using e-government services sites? (0-12, 12-17, 18-23, 24-30, more than 30)
- How long have you been using e-government services in Oman? (months) (0 – 5, 6-10, 11 – 15, 16-20, more than 20)
- Over the past 12 months, approximately how much have you paid via e-government sites for government services? (0, 0-100, 101-500, 500-1000, more than 1000)

*Items from Suh and Han (2003):*
- I frequently interact with the government through e-government services sites. (5 point Likert scale)

*Item developed for this study:*
- The best statement to describe my actual use of e-government services is
  - No use of e-government services sites at all.
  - To get government information only.
  - To get information and to conduct essential transactions only whenever there is no other way to get the service.
  - To get information and conduct transactions regularly.

5.4.2. **Questionnaire pre-testing**

Prior to the pilot testing stage the questionnaire underwent a pre-testing process to ensure the questionnaire contents and wording clarity. Ten Western Australian (WA) Omani students were used in this process. Ten copies of the questionnaire were printed and handed to the participants. The participants were asked to answer the questionnaire and to comment on its quality and clarity. The copies of the questionnaire and comments were collected after a week. Changes were made to the questionnaire based on the feedback. Copies were then sent electronically to three Arabic language
specialists in Oman to check the Arabic grammar and suitability of the words and construction of sentences. The questionnaire was then further modified based on the feedback from these specialists.

5.4.3. **Pilot study using questionnaire**

Oppenheim states “Pilot work can be of the greatest help in devising the actual wording of questions, and it operates as a healthy check, since fatal ambiguities may lurk in the most unexpected quarters” (Oppenheim, 1966, p. 26). A good questionnaire should avoid ambiguity and should address two main principles: clarity and keeping the participants’ perspective in mind (Neuman, 2003). A pilot study of the quantitative part of the study was therefore undertaken. Primarily, the pilot study aimed to address the following issues:

- Identify further areas in need of further clarity and rewording;
- Minimize any item redundancy;
- Examine the item sequence, flow and appropriateness;
- Minimize misunderstanding of questions;
- Measure the average time required to answer the questionnaire;
- Practise the data analysis process;
- Analyse the questionnaire as a tool serving the purpose data collection for the study.

The pilot study was undertaken using Omani citizens studying in WA universities and colleges. The participants in the pilot study were mostly employees in the Omani government; they can be viewed as a micro sample of the target sample for the research. More than 70 of the initial questionnaire forms were distributed and were requested back within a week. Participants were asked to complete the questionnaire and write any
comments about the questionnaire quality and clarity on the last page or at each spot they found appropriate. Each participant was asked to note down the starting and ending time when completing the questionnaire. Only 39 responses were received. These responses were from 26 men and 13 women.

Upon receiving the returned questionnaire forms with comments, feedback was considered and carefully integrated. Most of the comments were either about the clarity of the wording or about the length of the questionnaire. Several further changes were made to wording. The average time taken to fill in the questionnaire was 18.2 minutes which was considered acceptable (Alreck & Settle, 1995; Neuman, 2003; Oates, 2006; Rea & Parker, 2005). However in response to the feedback collected during the pilot study the number of items was reduced (see Section 5.4.1). Because it was the first study on e-privacy concerns in Oman, this questionnaire received many positive comments by many participants. Most of the participants were interested in seeing the results.

This phase was not only intended to test the quality of the questionnaire and the practicality of collecting data, but was also useful for the researcher to practise the required data analysis techniques. The data from the pilot study was stored in SPSS, and SPSS was used for the descriptive analysis. SmartPLS version 2.0 was used to obtain preliminary estimates of the reliability and validity of construct measurement (see Section 5.7.1). The results of this process are shown in Table 5.11. The results suggested that the questionnaire was suitable to use in the study. The low Cronbach alpha obtained for prior e-services experience (0.67) was assumed to be due to the limited number of participants at this stage.
<table>
<thead>
<tr>
<th>Construct</th>
<th>Average Variance Extracted</th>
<th>Composite Reliability</th>
<th>Cronbach Alpha</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-privacy awareness</td>
<td>0.55</td>
<td>0.82</td>
<td>0.71</td>
</tr>
<tr>
<td>E-privacy risk concerns</td>
<td>0.57</td>
<td>0.84</td>
<td>0.75</td>
</tr>
<tr>
<td>Perceived e-privacy protection</td>
<td>0.64</td>
<td>0.90</td>
<td>0.86</td>
</tr>
<tr>
<td>Prior e-services experience</td>
<td>0.51</td>
<td>0.80</td>
<td>0.67</td>
</tr>
<tr>
<td>Intention to use e-government services</td>
<td>0.62</td>
<td>0.89</td>
<td>0.85</td>
</tr>
<tr>
<td>Perceived usefulness of e-government services</td>
<td>0.55</td>
<td>0.83</td>
<td>0.72</td>
</tr>
<tr>
<td>Social norms</td>
<td>0.54</td>
<td>0.82</td>
<td>0.71</td>
</tr>
<tr>
<td>Perceived trustworthiness of e-government services</td>
<td>0.66</td>
<td>0.92</td>
<td>0.89</td>
</tr>
</tbody>
</table>

5.5. **Quantitative data collection procedures**

In the period from December 15, 2007 to March 15, 2008 the major survey was conducted. Eighteen key contact points (e.g. personnel managers and other senior administrators) were identified within 18 government units selected from the 45 units within the civil service sector. These contact points were responsible for distribution and collection of questionnaires. The key contact points distributed the questionnaires to potential participants. Participation in the questionnaire was clearly made optional and questionnaires were only distributed to volunteers. Form collection was through dedicated closed boxes at each government unit. An introductory letter was attached to the beginning of each questionnaire to introduce the study and inform the participants about the nature of the research, and to let them know that participation was voluntary and anonymous. The letter also indicated that submission of the completed questionnaire was taken as consent to use the data specifically for research related purposes (see page 2 of Appendix A).
A total of 700 questionnaire forms were distributed. There were 420 forms returned giving a response rate of 60%, however only 402 forms were usable as 18 of the returned forms had substantial missing data. Table 5.12 provides summary information about the government units included in the quantitative data collection and about the response rate from these units.

Table 5-12  Questionnaire distribution

<table>
<thead>
<tr>
<th>S#</th>
<th>Government Unit</th>
<th>Forms Distributed</th>
<th>Forms Returned</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Ministry of Civil Service</td>
<td>100</td>
<td>23</td>
</tr>
<tr>
<td>2.</td>
<td>Ministry of National Economy</td>
<td>30</td>
<td>20</td>
</tr>
<tr>
<td>3.</td>
<td>Ministry of National Heritage</td>
<td>25</td>
<td>19</td>
</tr>
<tr>
<td>4.</td>
<td>Ministry of Education</td>
<td>173</td>
<td>132</td>
</tr>
<tr>
<td>5.</td>
<td>Ministry of Higher Education</td>
<td>25</td>
<td>7</td>
</tr>
<tr>
<td>6.</td>
<td>Ministry of Oil and Gas</td>
<td>25</td>
<td>19</td>
</tr>
<tr>
<td>7.</td>
<td>Ministry of Health</td>
<td>25</td>
<td>13</td>
</tr>
<tr>
<td>8.</td>
<td>Ministry on Justice</td>
<td>25</td>
<td>17</td>
</tr>
<tr>
<td>9.</td>
<td>Ministry of Religions Affair</td>
<td>25</td>
<td>18</td>
</tr>
<tr>
<td>10.</td>
<td>Ministry of Transportation</td>
<td>10</td>
<td>8</td>
</tr>
<tr>
<td>11.</td>
<td>Ministry of Regional Municipalities</td>
<td>10</td>
<td>7</td>
</tr>
<tr>
<td>12.</td>
<td>Ministry of Housing</td>
<td>20</td>
<td>18</td>
</tr>
<tr>
<td>13.</td>
<td>Ministry of Man Power</td>
<td>25</td>
<td>15</td>
</tr>
<tr>
<td>14.</td>
<td>Ministry of Social Affairs</td>
<td>15</td>
<td>10</td>
</tr>
<tr>
<td>15.</td>
<td>Ministry of Agriculture</td>
<td>15</td>
<td>13</td>
</tr>
<tr>
<td>16.</td>
<td>Pension Funds</td>
<td>87</td>
<td>47</td>
</tr>
<tr>
<td>17.</td>
<td>National Crafts Authority</td>
<td>25</td>
<td>19</td>
</tr>
<tr>
<td>18.</td>
<td>Public Institute of Administration</td>
<td>40</td>
<td>15</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>700</td>
<td>420</td>
</tr>
<tr>
<td>Percentage</td>
<td></td>
<td>100%</td>
<td>60%</td>
</tr>
</tbody>
</table>
5.6. Qualitative data collection procedures

Interviews as a data gathering approach are used in many aspects of our lives. The physician interviews the patient to diagnose the illness, employers select their new employees’ mostly through interviews and a similar process occurs in many other aspects of life. Survey by interview plays an essential role in qualitative research. Therefore a survey using interviews was used a second data collection approach in this study.

The qualitative survey in this study was conducted using semi-structured interviews. The interviews were intended to seek qualitative data regarding the impact of e-privacy concerns on citizens’ intention to use e-government services. The interviews were to allow participants to provide their views and to further elaborate on the research subject. They were meant to complement the questionnaire by collecting specific details that could not be captured by questionnaire and as a way of asking the questions differently.

Interview participants were identified as a result of their willingness to be interviewed as noted on the questionnaire forms or were identified by the researcher. All participants were then contacted to agree on a suitable interview time and venue. Interviews were conducted at places of the participants’ choice. Some of the interviews took place at the participants’ offices, others at participants’ houses or coffee shops of their selection. All interviews were carried out during the period January 13-31, 2008. Participants first signed a consent form that guaranteed confidentiality. The interviewer used a pre-prepared list of questions (interview guide). The interview guide was used to help the researcher to sequence the questions and to keep him on track during the interview’s dialogue. All research constructs were considered in the interview guide. The guide started with questions to obtain the participant’s demographic information.
Then guide went into the status of e-government use in Oman followed by a number of questions related to the concepts and constructs of the research (see Appendix C).

A total of 19 interviews were conducted. All but one of the interviews were digitally recorded (one participant preferred not to have their interview recorded). The average interview length was 28.59 minutes with a range from 11.04 minutes to 52.34 minutes. The interviews were digitally recorded, indexed, timed and dated within the recorder. All recorded conversations then were hand transcribed into English while listening to the recorded voice. The process was repeated three times just to make sure that correct transcription was done. The hand written transcripts were then tabulated using Microsoft Word tables. Each interview was tabulated in an interview sheet. Each interview was assigned a number from 1-19, which was recorded on the interview sheet to be used for future reference. The unrecorded interview was also transcribed and tabulated using the same process. Each transcribed sheet contained three columns. The first column showed the guide question number. The second column described the question asked of the participant. The third column captured the participant’s response to the question.

5.7. Data analysis

This section describes the data analysis techniques chosen to support the research. As previously mentioned, the questionnaire was used to collect data for the quantitative part of this study and the interviews were used as the basis for the qualitative part. The quantitative part used partial least squares (PLS) to test the model. Smart PLS version 2.0 was used in this research. The quantitative analysis was also undertaken using SPSS version 15.0 for Windows to store the collected data and to produce the descriptive statistics. The qualitative part of the analysis used Microsoft Word to support concept
extraction and grouping. Concepts extraction basically depended on theme generation, theme coding, and data interpretation.

5.7.1. **Quantitative data analysis**

As stated above, this study used Smart PLS to examine the research model. PLS is an alternative approach to traditional structural equation modelling, and has been used widely in information systems research. It is a method that is designed to maximize prediction rather than fit (Fornell & Bookstein, 1982). PLS was used to study the validity of the model’s main components and to determine the relationships among the constructs of the proposed model.

According to Fornell and Bookstein (1982) and Hulland (1999), PLS is usually used as an analytical tool in two sequential steps; these are assessment of the validity of the measurement model and then assessment of the structural model. This two-step approach was adopted for the testing of the proposed model. In this approach, the fit and construct validity of the proposed measurement model are tested first. Once a satisfactory measurement model is obtained, the measurement model is “fixed” when the structural model is estimated. Through this technique overall reliability and validity are usually assured (Hair, Anderson, Tatham, & Black, 2006).

5.7.1.1. **Measurement (outer) model assessment**

The measurement model was assessed in terms of convergent validity and discriminant validity. Convergent validity is shown when each measurement item correlates strongly with its proposed construct (Gefen & Straub, 2005). Convergent validity was assessed using item loadings and their significance, composite reliability, Cronbach alpha, and average variance extracted (AVE). When the criteria established to assess convergent
validity are met then the items are said to be convergent on the proposed latent construct. These criteria are shown in Table 5.13.

Table 5-13 Criteria used for convergent validity

<table>
<thead>
<tr>
<th>Convergent validity criteria</th>
<th>Guideline</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item loadings</td>
<td>&gt;=0.70</td>
<td>Hulland (1999)</td>
</tr>
<tr>
<td>Composite reliability</td>
<td>&gt;=0.70</td>
<td>Hair et al. (1995)</td>
</tr>
<tr>
<td>Average variance extracted</td>
<td>&gt;=0.50</td>
<td>Hair et al. (1995)</td>
</tr>
<tr>
<td>Cronbach alpha coefficient</td>
<td>&gt;=0.70</td>
<td>Gefen &amp; Straub (2005)</td>
</tr>
<tr>
<td>t-value of outer loading</td>
<td>&gt;=1.96</td>
<td>Gefen &amp; Straub (2005)</td>
</tr>
</tbody>
</table>

Measurement items which did not load satisfactorily on their constructs (>0.7), were dropped from the model. The t-values of the outer loadings were also tested to ensure that each item loaded significantly on its latent variable.

Composite reliability was used to assess the internal consistency of the measurement model. Composite reliability is a general measure of reliability that uses the item loadings estimated within the model. Composite reliability should be at least 0.7 to be accepted (Hair et al., 1995).

Cronbach alpha is used to measure the inter-correlation among items in a group indicating to what level the items are measuring a single latent variable. In PLS composite reliability is often used instead of Cronbach alpha when validating the measurement model. Both were included in this analysis. Cronbach alpha can be
interpreted similarly to composite reliability and values of at least 0.7 are considered acceptable (Hair et al., 1995).

AVE reflects the overall amount of variance in the indicators accounted for by the latent construct. AVE should be more than 0.5 to be considered acceptable (Hair et al., 1995).

The measurement model was also assessed in terms of discriminant validity. Discriminant validity validates that each measurement item correlates weakly with all other constructs except for the one with which it is proposed to be associated.

Discriminant validity in PLS is tested by comparing AVE and inter-construct correlations. This is done in two steps:

- Comparing item cross loadings to construct correlations;
- Examining the ratio of the square root of the AVE of each construct to the correlations of this construct with all other constructs (Gefen & Straub, 2005).

For satisfactory discriminant validity each item should load more highly on its own construct than on other constructs. In addition, the average variance shared between a construct and its measures should be greater than the variance shared by the construct and any other constructs in the model (Gefen & Straub, 2005).
5.7.1.2. **Structural (inner) model assessment**

The structural model is tested to evaluate interrelationships of the constructs. In this study the structural model was evaluated on two criteria:

- The ability to explain variance in the dependent variables;
- The significance of the path coefficients.

An estimate of the variance explained the dependent variables is provided by the squared multiple correlations ($R^2$) of the structural equations of these variables. $R^2$ was used as an estimate of how much of the variability of a dependent variable is explained by the independent variables (Hair et al., 1995).

For the second evaluation criteria, the structural model was evaluated on whether it reflects valid interrelationships by testing the t-values of the proposed relationships (Hair et al., 1995). Smart PLS provides path coefficients that indicate the strength of the relationship between two constructs. The bootstrap procedures with 500 re-sample were used to calculate the significance of these path coefficients. In addition to the significance of the path coefficients, the strengths of the relationships they represent were also of interest. In this study correlations of less than 0.2 were considered weak, correlations between 0.2 to 0.5 were considered to be moderate, and correlations of more than 0.5 were considered to be strong (Cohen, 1988).

5.7.2. **Qualitative data analysis**

The qualitative data analysis in this study depended on interview data analysis. Interview analysis is the mechanism of processing raw interview data, most likely recorded voice or another format of captured interview data, to produce evidence based interpretations that can be represented in a standard academic report (Silverman, 1993).
It is not only the process of collecting, coding, sorting, and sifting but it also covers the process of noticing, categorizing, contrasting, weighing, and merging results to develop meaning and implications of patterns (Seidel, 1998). Interviews conducted in this study yielded digital voice recorded data. A qualitative data analysis took place which involved abstracting the data that was related to the main variables and themes of the research. The qualitative analysis in this study adopted the technique described by Dey (1993) and Silverman (1993). This qualitative data was analysed to compliment the quantitative findings using the procedures described below.

The analysis started by examining all the interview transcripts to identify concepts and themes associated with the constructs from the proposed model. Since the interviews were semi-structured and the interview guide was built around the research main constructs, it was easy to identify themes related to the constructs. Synonyms for constructs were identified and used in theme extraction. For example, terms such as “risk threats” and “risk concerns” were used to identify themes around e-privacy risk concerns. This process was carried out to identify all concepts and themes in all transcribed responses and was undertaken using Microsoft Word capabilities such as word searching, using Word’s search facility and highlighting text in multiple colours.

Data then was categorized according to the identified themes. Because the interview questions were structured directly around the research constructs and their relationships as proposed in the model, it was relatively straightforward to classify responses related to identified themes against each research construct as shown in Appendix D. Microsoft Word was used to present this classification in table format.
Portions of the responses that were not related to the research constructs were classified as either participants’ background data or general data. The background data about the participants was compiled to describe the backgrounds of the participants in the interviews. The general data that was not specifically related to the research model was retained for later further analysis.

The fourth step in the process was to further analyse the data relating to the research model. The responses relating to each construct (see Appendix D) were synthesised as shown in Appendix E and Appendix F. These synthesised findings were used to reflect the participants’ views on the research constructs and their relationships. This step enabled the researcher to map responses together within one consolidated table and examine them in-depth to identify where there was consensus and where opinions varied. Conclusions were drawn based on this.

The final step in the process was to utilize the analysis from previous steps (see Appendix E and Appendix F) to link the synthesised responses to each research hypothesis. Appendix G shows each proposed hypothesis and the support (or lack of support) for it from the interview findings.

5.8. Summary

This chapter described the research methodology used in the study. This research was conducted using quantitative and qualitative approaches. The quantitative approach was carried out via questionnaire and the qualitative approach was undertaken through semi-structured interviews. The chapter explained the reasons for the selection of these methods and provides details of how the participants were selected. The chapter also explained how the questionnaire and interview questions were designed and the data
analysis approaches used. The next chapter presents the results of the quantitative testing of the research model.
Chapter 6. Quantitative Findings

6.1. Introduction

This chapter reports on the results of the quantitative data collection and analysis that were carried out as described in Chapter 5. The questionnaire was designed to collect the quantitative data required to understand the impact of e-privacy risk concerns and other factors, as discussed in Chapter 4, on citizens’ intentions to use e-government services in Oman. Section 6.2 presents descriptive information about the participants and their actual use of e-government services. Section 6.3 discusses the measurement model testing and this is followed by a discussion of the test of the structural model in Section 6.4. The outcomes of the hypothesis testing are presented in Section 6.5. Section 6.6 presents an assessment of the strengths of the proposed relationships and Section 6.7 discusses the total effects. The chapter then concludes in Section 6.8 with some additional insights based on comments provided by the respondents.

6.2. Descriptive statistics

This section provides background information about the participants and describes their actual e-government services use. As previously mentioned in Chapter 5 a total of 420 questionnaires out of 700 were completed and returned. The response rate was 60%. Only 402 questionnaires were found to be usable as those with high rate of missing data were excluded from the analysis.

6.2.1. User profile

Of the respondents who provided information about their gender, 150 (37.9%) were female and 246 were male (62.1%). This information allows the participants to be compared with the distribution of employees in the civil service sector. According to the
Ministry of Civil Service Employees statistics report of June 30, 2007 (Ministry of Civil Service, 2007), females formed about 39% of total government employees, therefore the gender balance of participants is consistent with that of the civil service sector.

Table 6.1 shows the overall participants’ age distributions. The largest category of respondents was those between 18 and 29 years of age (52.7%), followed by those in the 30 to 49 age range (46.6%). There were only three respondents who were 50 or over in age. The workforce in the civil sector is predominantly young with 60 being the oldest age for employees (Ministry of Civil Service, 2007), but nevertheless it seems that younger people were more interested in the subject of the research and hence more likely to participate.

Table 6-1 Age distribution

<table>
<thead>
<tr>
<th>Age ranges</th>
<th>Categories</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>18 - 29</td>
<td>208</td>
<td>52.7</td>
<td></td>
</tr>
<tr>
<td>30 - 49</td>
<td>184</td>
<td>46.6</td>
<td></td>
</tr>
<tr>
<td>50+</td>
<td>3</td>
<td>0.7</td>
<td></td>
</tr>
</tbody>
</table>

Table 6.2 below shows the educational background of the participants. The vast majority of the respondents (92%) held at least a college degree. This high proportion raises the question of whether degree holders were more interested in the topic and hence more likely to participate. Only 7.2% of respondents had high school or less as their educational background.
Table 6-2 Educational background

<table>
<thead>
<tr>
<th>Categories</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>High school or less</td>
<td>29</td>
<td>7.3</td>
</tr>
<tr>
<td>Some college</td>
<td>72</td>
<td>18.0</td>
</tr>
<tr>
<td>College graduate</td>
<td>259</td>
<td>65.0</td>
</tr>
<tr>
<td>Postgraduate</td>
<td>39</td>
<td>9.8</td>
</tr>
</tbody>
</table>

Table 6.3 below illustrates the participants’ Internet and e-service use background. Responses indicated that 83.3% of the participants believed that they had intermediate to advanced levels of Internet experience compared with 15.4% who believed they were beginners. Only 1.2% of the participants had no Internet experience. The responses also indicated that 66% of the participants had at least intermediate levels of experience with e-services and 26.2% of the participants believed that they had beginner levels of e-service experience. Only 7.8% of the participants who had no e-service experience at all.

Table 6-3 Internet and e-service background

<table>
<thead>
<tr>
<th>None</th>
<th>Beginner</th>
<th>Intermediate</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Count</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1.2</td>
<td>62</td>
<td>15.4</td>
</tr>
<tr>
<td>249</td>
<td>61.9</td>
<td>86</td>
<td>21.4</td>
</tr>
<tr>
<td>31</td>
<td>7.8</td>
<td>105</td>
<td>26.2</td>
</tr>
<tr>
<td>201</td>
<td>50</td>
<td>64</td>
<td>16</td>
</tr>
</tbody>
</table>

Table 6.4 below reports the participants’ ICT training background. A majority of participants reported having had previous ICT training (65.1%). A total of 34.9% stated
they had not had any previous ICT training. Similar percentages of females and males had received ICT training (64.9% versus 65.3%) These figures suggest that ICT training in Oman is equally available to civil service employees of both genders.

Table 6-4 Previous ICT training

<table>
<thead>
<tr>
<th>Item</th>
<th>Categories</th>
<th>Female Count</th>
<th>Female Percent</th>
<th>Male Count</th>
<th>Male Percentage</th>
<th>Total Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Previous ICT training?</td>
<td>Yes</td>
<td>96</td>
<td>64.9</td>
<td>160</td>
<td>65.3</td>
<td>65.1</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>52</td>
<td>35.1</td>
<td>85</td>
<td>34.7</td>
<td>34.9</td>
</tr>
</tbody>
</table>

6.2.2. Use of e-government services

This section describes the level and nature of e-government use in Oman at the time the survey was conducted. As shown in Table 6.5 below, slightly more than 29% of participants said that they had never used e-government services. About 39% of the participants stated that they used e-government services for information searches but not for online transactions, and 18.2% used e-government sites only when there was no other way to conduct the transaction. Very few participants (12.5%) reported regular use of e-government services.

Table 6-5 Level of e-government services use

<table>
<thead>
<tr>
<th>Level of e-government services use</th>
<th>No use</th>
<th>For information</th>
<th>If no other way</th>
<th>Always</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Count</td>
<td>Percent</td>
<td>Count</td>
<td>Percent</td>
</tr>
<tr>
<td></td>
<td>117</td>
<td>29.9</td>
<td>154</td>
<td>39.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>71</td>
<td>18.2</td>
</tr>
<tr>
<td></td>
<td>49</td>
<td>12.5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 6.6 below categorizes the length of time in months that citizens had been using e-government services. The majority of participants (78.2%) had used e-government services for less than two years. Only 21.8% reported that they had used e-government services for more than two years.

Table 6-6  Period of e-government services usage

<table>
<thead>
<tr>
<th>Length of time using e-government services (months)</th>
<th>Categories</th>
<th>Count</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - 12</td>
<td>222</td>
<td>56.4</td>
<td></td>
</tr>
<tr>
<td>12 - 17</td>
<td>54</td>
<td>13.7</td>
<td></td>
</tr>
<tr>
<td>18 - 23</td>
<td>32</td>
<td>8.1</td>
<td></td>
</tr>
<tr>
<td>24 - 30</td>
<td>39</td>
<td>9.9</td>
<td></td>
</tr>
<tr>
<td>30 +</td>
<td>47</td>
<td>11.9</td>
<td></td>
</tr>
</tbody>
</table>

Table 6.7 below reports the amount of time in hours that participants spent using e-government services each month. The largest group (77%) reported that they spent five or less hours a month using e-government services, and 13.1% spent between five and 10 hours a month. Only 9.9% used e-government services for more than 10 hours a month.

Table 6-7  E-government services usage in hours

<table>
<thead>
<tr>
<th>Hours spent using e-government services each month</th>
<th>Categories</th>
<th>Count</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - 5</td>
<td>304</td>
<td>77.0</td>
<td></td>
</tr>
<tr>
<td>6 - 10</td>
<td>52</td>
<td>13.1</td>
<td></td>
</tr>
<tr>
<td>11 - 15</td>
<td>17</td>
<td>4.3</td>
<td></td>
</tr>
<tr>
<td>16 - 20</td>
<td>11</td>
<td>2.8</td>
<td></td>
</tr>
<tr>
<td>20+</td>
<td>11</td>
<td>2.8</td>
<td></td>
</tr>
</tbody>
</table>
Table 6.8 below reports on the respondents’ personal information disclosure to e-government sites, and their use of e-government sites for payment. It shows that the largest group of participants (45.7%) had never disclosed their personal information to the government using e-government sites, and that 23.7% of them rarely disclosed their personal information to e-government sites. Nearly 21% regularly disclosed personal information to e-government sites. Only about 9.8% of participants said that they usually or always disclosed their personal information to e-government sites.

Table 6-8 Personal information disclosure and payment

<table>
<thead>
<tr>
<th>Disclosure of personal information to e-government sites</th>
<th>Never before</th>
<th>Seldom</th>
<th>About half the time</th>
<th>Usually</th>
<th>Always</th>
</tr>
</thead>
<tbody>
<tr>
<td>Count</td>
<td>Percent</td>
<td>Count</td>
<td>Percent</td>
<td>Count</td>
<td>Percent</td>
</tr>
<tr>
<td>181</td>
<td>45.7</td>
<td>94</td>
<td>23.7</td>
<td>82</td>
<td>20.7</td>
</tr>
</tbody>
</table>

| Payment through e-government sites | 282 | 71.2 | 57 | 14.4 | 37 | 9.4 | 15 | 3.8 | 4 | 1.0 |

The second row of Table 6.8 above reports the frequency of participants’ payment through e-government sites. Participants were even less likely to make payments through e-government sites than they were to provide personal information. A majority of the participants (71.2%) reported that they had never paid for services through e-government sites, and only 4.8% usually or always used e-government sites to pay for government services.
Table 6.9 below describes the amounts that participants had paid via e-government services in the last 12 months. Not surprisingly, 79.4% reported that they did not use e-government services at all for payments and 18% stated that they only spent 1-100 Omani Rials (AUD 4.0). Only 2% of the participants indicated that they spent 101-500 Omani Rial in the last 12 months and just 0.5% stated that they spent above 500 Omani Rials during the last year. These figures are consistent with the results reported in the previous tables in that levels of use of e-government services are relatively low, and citizens are starting with activities that would be perceived as low risk, such as obtaining information, rather than using the services for making payments.

<table>
<thead>
<tr>
<th>Categories</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>313</td>
<td>79.4%</td>
</tr>
<tr>
<td>1 - 100</td>
<td>71</td>
<td>18.0%</td>
</tr>
<tr>
<td>101 - 500</td>
<td>8</td>
<td>2.0%</td>
</tr>
<tr>
<td>500–1000</td>
<td>2</td>
<td>0.5%</td>
</tr>
<tr>
<td>1000+</td>
<td>0</td>
<td>0%</td>
</tr>
</tbody>
</table>

6.2.3. Summary information on the research constructs

Table 6.10 below provides summary information about the research constructs. The responses to the items used measure each construct were averaged for each participant, and descriptive information about these summary measures of the main constructs is provided to give a sense of overall level and spread. All constructs showed a wide range of values. The table clearly shows that the majority of participants perceived that e-government services in Oman will be very useful to them (mean: 2.78 out of 5). It was also clear that most participants were very concerned about risks to their e-privacy in
relation to using e-government services (mean: 4.10 out of 5). Consistent with the results shown in Table 6.3 prior e-services experience levels were intermediate (mean: 4.20 out of 5). In regard to e-privacy awareness, the data shows that there was a wide range of levels of awareness, however, on average the participants had reasonable levels of awareness of e-privacy issues (mean: 3.30 out of 5). Similarly, there was a very wide range of levels of perceived trustworthiness and of social norms. Finally, the table shows that a substantial number of participants were not sure about their future intentions, though the tendency was towards intending to use e-government services (mean: 3.80 out of 5).

Table 6-10  Construct summary information

<table>
<thead>
<tr>
<th>Construct</th>
<th>Mean</th>
<th>Min</th>
<th>Max</th>
<th>Std</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perceived usefulness of e-government services</td>
<td>4.20</td>
<td>2.7</td>
<td>5</td>
<td>0.48</td>
</tr>
<tr>
<td>Social norms</td>
<td>3.79</td>
<td>1</td>
<td>5</td>
<td>0.59</td>
</tr>
<tr>
<td>Prior e-services experience</td>
<td>2.78</td>
<td>1</td>
<td>5</td>
<td>0.87</td>
</tr>
<tr>
<td>E-privacy risk concerns</td>
<td>4.10</td>
<td>2.2</td>
<td>5</td>
<td>0.54</td>
</tr>
<tr>
<td>E-privacy awareness</td>
<td>3.30</td>
<td>1</td>
<td>5</td>
<td>0.82</td>
</tr>
<tr>
<td>Perceived e-privacy protection</td>
<td>3.50</td>
<td>1.4</td>
<td>5</td>
<td>0.71</td>
</tr>
<tr>
<td>Perceived trustworthiness of e-government services</td>
<td>3.10</td>
<td>1</td>
<td>5</td>
<td>0.70</td>
</tr>
<tr>
<td>Intention to use e-government services</td>
<td>3.80</td>
<td>1.8</td>
<td>5</td>
<td>0.55</td>
</tr>
</tbody>
</table>

6.3.  Testing the measurement model

The criteria discussed in Chapter 5 were used to validate the measurement model. Two main aspects of validity were considered: convergent and discriminant validity. This section demonstrates how both were achieved.
6.3.1.  **Convergent validity**

Convergent validity is satisfied when each measurement item correlates strongly with its proposed construct (Gefen & Straub, 2005). Figure 6.1 below presents the initial measurement model as produced by SmartPLS. It shows the initial items loadings on their constructs. Appendix H shows the complete list of measurement items that were used in this assessment and their labels.

![The measurement model](image)

**Figure 6.1 The measurement model**

The first aspect of the model evaluated was item loadings. Table 6.11 below lists the initial outer loading value for each item in relation to its latent variable.
According to Hulland (1999) item loadings should be more than 0.7. All items that did not meet this criterion were dropped from the model as listed in Table 6.12 below. Therefore, the remaining items satisfy the first criterion of convergent validity. Each construct is discussed below.
<table>
<thead>
<tr>
<th>Item</th>
<th>Loading</th>
<th>Item</th>
<th>Loading</th>
<th>Item</th>
<th>Loading</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aware2</td>
<td>0.82</td>
<td>Intent5</td>
<td>0.87</td>
<td>Trust2</td>
<td>0.71</td>
</tr>
<tr>
<td>Aware3</td>
<td>0.86</td>
<td>Protec1</td>
<td>0.74</td>
<td>Trust3</td>
<td>0.85</td>
</tr>
<tr>
<td>Aware4</td>
<td>0.75</td>
<td>Protec2</td>
<td>0.80</td>
<td>Trust4</td>
<td>0.81</td>
</tr>
<tr>
<td>Con1</td>
<td>0.82</td>
<td>Protec3</td>
<td>0.75</td>
<td>Trust5</td>
<td>0.75</td>
</tr>
<tr>
<td>Con2</td>
<td>0.87</td>
<td>Protec4</td>
<td>0.77</td>
<td>Trust6</td>
<td>0.84</td>
</tr>
<tr>
<td>Con4</td>
<td>0.79</td>
<td>Protec5</td>
<td>0.71</td>
<td>Use4</td>
<td>0.85</td>
</tr>
<tr>
<td>Exper1</td>
<td>0.81</td>
<td>S_nor1</td>
<td>0.79</td>
<td>Use5</td>
<td>0.88</td>
</tr>
<tr>
<td>Exper2</td>
<td>0.80</td>
<td>S_nor2</td>
<td>0.85</td>
<td>Use6</td>
<td>0.82</td>
</tr>
<tr>
<td>Exper3</td>
<td>0.80</td>
<td>S_nor3</td>
<td>0.85</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exper5</td>
<td>0.81</td>
<td>S_nor4</td>
<td>0.78</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intent3</td>
<td>0.77</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intent4</td>
<td>0.89</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Perceived usefulness of e-government services**

Only three items of the six items measuring perceived usefulness of e-government services (Use) loaded sufficiently on the construct. The other items were dropped as they did not meet the criteria.

**Social norms**

Analysis of the social norms (S_nor) construct showed that all of the four items reflected the measured construct of social norms. All items were therefore retained.

**Prior e-services experience**

Four out of the items used to measure prior e-service experience (Exper), had outer loadings of more than 0.7. One item (Exper4) was 0.63 therefore it was dropped as it did not meet the criteria. The rest of the items were considered to be good indicators of
prior e-service experience and the construct satisfied this requirement for convergent reliability.

**E-privacy risk concerns**

Only three items out of the eight loaded at more than 0.7 on the construct e-privacy risk concerns (Con). Items Con3, Con5, Con6, Con7, and Con8 had measurements of 0.6 or less therefore they were dropped.

**E-privacy awareness**

Analysis of the e-privacy awareness (Aware) construct shows that the item Aware1 was below the accepted loading with a value of 0.47, it was therefore dropped.

**Perceived e-privacy protection**

All items loadings of perceived e-privacy protection (Protec) were above 0.7 the items therefore were considered to be good indicators of the perceived e-privacy protection construct.

**Perceived trustworthiness of e-government services**

All items loadings of perceived trustworthiness of e-government services (Trust) were above 0.7 and thus satisfied the criteria. The items therefore were considered to be good indicators of trustworthiness in e-government services.

**Intention to use e-government services**

Two items used to measure intention to use e-government services (Intent) were below 0.7 (Intent1 and Intent2) and were therefore dropped. The other 3 items loaded at greater than 0.7 so were retained.
The t values of the outer loadings were also tested for the remaining items, to ensure that each item loaded significantly on its latent variable. Table 6.13 below shows that all items loaded significantly on their constructs.

The third criterion of convergent validity evaluated was composite reliability. Table 6.14 below shows that all values of composite reliability were more than 0.70. Therefore they demonstrated the internal consistency of the constructs in the measurement model.

The fourth convergent validity criterion assessed was Cronbach alpha which is used to measure the reliability of a set of two or more construct indicators. Cronbach alpha should be at values above 0.7. Table 6.14 shows the Cronbach alpha values for each construct in the model. All values were greater than 0.7 and therefore meet the requirements.
Table 6-13  Outer loading bootstrap analysis

<table>
<thead>
<tr>
<th>Item Association</th>
<th>Mean</th>
<th>Std. dev.</th>
<th>t value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aware2 ← E-privacy awareness</td>
<td>0.82</td>
<td>0.04</td>
<td>20.05***</td>
</tr>
<tr>
<td>Aware3 ← E-privacy awareness</td>
<td>0.85</td>
<td>0.03</td>
<td>25.52***</td>
</tr>
<tr>
<td>Aware4 ← E-privacy awareness</td>
<td>0.75</td>
<td>0.06</td>
<td>12.35***</td>
</tr>
<tr>
<td>Con1 ← E-privacy risk concerns</td>
<td>0.81</td>
<td>0.03</td>
<td>23.48***</td>
</tr>
<tr>
<td>Con2 ← E-privacy risk concerns</td>
<td>0.86</td>
<td>0.03</td>
<td>32.39***</td>
</tr>
<tr>
<td>Con4 ← E-privacy risk concerns</td>
<td>0.80</td>
<td>0.04</td>
<td>21.05***</td>
</tr>
<tr>
<td>Exper1 ← Prior e-services experience</td>
<td>0.79</td>
<td>0.14</td>
<td>5.92***</td>
</tr>
<tr>
<td>Exper2 ← Prior e-services experience</td>
<td>0.76</td>
<td>0.15</td>
<td>5.45***</td>
</tr>
<tr>
<td>Exper3 ← Prior e-services experience</td>
<td>0.76</td>
<td>0.14</td>
<td>5.57***</td>
</tr>
<tr>
<td>Exper5 ← Prior e-services experience</td>
<td>0.77</td>
<td>0.12</td>
<td>6.81***</td>
</tr>
<tr>
<td>Intent3 ← Intention to use e-government services</td>
<td>0.77</td>
<td>0.03</td>
<td>28.89***</td>
</tr>
<tr>
<td>Intent4 ← Intention to use e-government services</td>
<td>0.89</td>
<td>0.02</td>
<td>54.64***</td>
</tr>
<tr>
<td>Intent5 ← Intention to use e-government services</td>
<td>0.87</td>
<td>0.02</td>
<td>50.11***</td>
</tr>
<tr>
<td>Protec1 ← Perceived e-privacy protection</td>
<td>0.73</td>
<td>0.03</td>
<td>23.19***</td>
</tr>
<tr>
<td>Protec2 ← Perceived e-privacy protection</td>
<td>0.80</td>
<td>0.02</td>
<td>32.34***</td>
</tr>
<tr>
<td>Protec3 ← Perceived e-privacy protection</td>
<td>0.75</td>
<td>0.04</td>
<td>20.39***</td>
</tr>
<tr>
<td>Protec4 ← Perceived e-privacy protection</td>
<td>0.77</td>
<td>0.03</td>
<td>28.72***</td>
</tr>
<tr>
<td>Protec5 ← Perceived e-privacy protection</td>
<td>0.71</td>
<td>0.05</td>
<td>14.85***</td>
</tr>
<tr>
<td>S_nor1 ← Social norms</td>
<td>0.79</td>
<td>0.03</td>
<td>28.50***</td>
</tr>
<tr>
<td>S_nor2 ← Social norms</td>
<td>0.84</td>
<td>0.03</td>
<td>33.34***</td>
</tr>
<tr>
<td>S_nor3 ← Social norms</td>
<td>0.85</td>
<td>0.02</td>
<td>40.80***</td>
</tr>
<tr>
<td>S_nor4 ← Social norms</td>
<td>0.78</td>
<td>0.03</td>
<td>24.77***</td>
</tr>
<tr>
<td>Trust3 ← Perceived trustworthiness of e-government services</td>
<td>0.85</td>
<td>0.02</td>
<td>50.39***</td>
</tr>
<tr>
<td>Trust2 ← Perceived trustworthiness of e-government services</td>
<td>0.71</td>
<td>0.03</td>
<td>23.26***</td>
</tr>
<tr>
<td>Trust4 ← Perceived trustworthiness of e-government services</td>
<td>0.81</td>
<td>0.02</td>
<td>33.04***</td>
</tr>
<tr>
<td>Trust5 ← Perceived trustworthiness of e-government services</td>
<td>0.75</td>
<td>0.03</td>
<td>25.97***</td>
</tr>
<tr>
<td>Trust6 ← Perceived trustworthiness of e-government services</td>
<td>0.84</td>
<td>0.02</td>
<td>40.84***</td>
</tr>
<tr>
<td>Use4 ← Perceived usefulness of e-government services</td>
<td>0.85</td>
<td>0.02</td>
<td>43.77***</td>
</tr>
<tr>
<td>Use5 ← Perceived usefulness of e-government services</td>
<td>0.88</td>
<td>0.02</td>
<td>55.72***</td>
</tr>
<tr>
<td>Use6 ← Perceived usefulness of e-government services</td>
<td>0.82</td>
<td>0.02</td>
<td>37.06***</td>
</tr>
</tbody>
</table>

***p <0.001
Table 6-14 Convergent validity measures

<table>
<thead>
<tr>
<th>Construct</th>
<th>AVE</th>
<th>Composite Reliability</th>
<th>Cronbach alpha</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-privacy awareness</td>
<td>0.66</td>
<td>0.85</td>
<td>0.74</td>
</tr>
<tr>
<td>E-privacy risk concerns</td>
<td>0.69</td>
<td>0.87</td>
<td>0.77</td>
</tr>
<tr>
<td>Prior e-services experience</td>
<td>0.65</td>
<td>0.88</td>
<td>0.82</td>
</tr>
<tr>
<td>Intention to use e-government services</td>
<td>0.71</td>
<td>0.88</td>
<td>0.80</td>
</tr>
<tr>
<td>Perceived e-privacy protection</td>
<td>0.57</td>
<td>0.87</td>
<td>0.81</td>
</tr>
<tr>
<td>Social norms</td>
<td>0.67</td>
<td>0.89</td>
<td>0.83</td>
</tr>
<tr>
<td>Perceived trustworthiness of e-government services</td>
<td>0.63</td>
<td>0.90</td>
<td>0.85</td>
</tr>
<tr>
<td>Perceived usefulness of e-government services</td>
<td>0.72</td>
<td>0.89</td>
<td>0.81</td>
</tr>
</tbody>
</table>

The last convergent validity criteria assessed was AVE. As shown in Table 6.14 above, all values of AVE were more than 0.5 which is considered satisfactory. Therefore this convergent validity criterion was also met.

The analysis of all five of the established convergent validity criteria demonstrated evidence of convergent validity. Discriminant validity was then examined.

6.3.2. Discriminant validity

Discriminant validity, as previously mentioned, is shown when each item correlates weakly with all constructs except for the one it is theoretically associated with. As stated in Chapter 5 a construct should share more variance with its measures than it shares with other constructs in the proposed model. Discriminant validity measurement took place in two steps as shown below.
The first step involved examining the indicators’ cross loadings on their corresponding construct. Table 6.15 below lists the cross loadings measurements for each item. By examining the shaded loadings, where each group is for a single construct, it is clear that all values are larger than the rest of values within the same column and row. Thus loadings of items on their constructs were higher than cross loadings and therefore the first criterion is met.

The second step in testing discriminant validity was to check the square root of AVE of each construct and the associated correlations. Table 6.16 below provides the construct inter-correlations and the square root of average variance extracted for each construct (in bold on the diagonal). In all cases the square root of average variance extracted exceeds the corresponding construct inter-correlations thereby demonstrating discriminant validity. Therefore, both of the steps supported the discriminant validity of the measurement model.
Table 6-15 Table of cross loadings

<table>
<thead>
<tr>
<th>Item</th>
<th>E-privacy awareness</th>
<th>E-privacy risk concerns</th>
<th>Prior e-services experience</th>
<th>e-government services</th>
<th>Intention to use e-government services</th>
<th>Perceived e-privacy protection</th>
<th>Perceived trustworthiness of e-government services</th>
<th>Perceived usefulness of e-government services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aware2</td>
<td>0.82</td>
<td>0.21</td>
<td>0.06</td>
<td>-0.05</td>
<td>-0.22</td>
<td>-0.01</td>
<td>-0.20</td>
<td>0.06</td>
</tr>
<tr>
<td>Aware3</td>
<td>0.86</td>
<td>0.23</td>
<td>0.04</td>
<td>-0.13</td>
<td>-0.25</td>
<td>-0.01</td>
<td>-0.22</td>
<td>0.04</td>
</tr>
<tr>
<td>Aware4</td>
<td>0.75</td>
<td>0.21</td>
<td>0.01</td>
<td>-0.05</td>
<td>-0.14</td>
<td>-0.10</td>
<td>-0.14</td>
<td>0.00</td>
</tr>
<tr>
<td>Con1</td>
<td>0.19</td>
<td>0.82</td>
<td>0.05</td>
<td>-0.29</td>
<td>-0.16</td>
<td>-0.08</td>
<td>-0.17</td>
<td>-0.05</td>
</tr>
<tr>
<td>Con2</td>
<td>0.23</td>
<td>0.87</td>
<td>-0.05</td>
<td>-0.28</td>
<td>-0.21</td>
<td>-0.14</td>
<td>-0.21</td>
<td>-0.08</td>
</tr>
<tr>
<td>Con4</td>
<td>0.24</td>
<td>0.79</td>
<td>-0.03</td>
<td>-0.21</td>
<td>-0.10</td>
<td>-0.06</td>
<td>-0.20</td>
<td>0.01</td>
</tr>
<tr>
<td>Exper1</td>
<td>0.04</td>
<td>-0.07</td>
<td>0.81</td>
<td>0.23</td>
<td>0.06</td>
<td>0.24</td>
<td>0.11</td>
<td>0.18</td>
</tr>
<tr>
<td>Exper2</td>
<td>0.04</td>
<td>0.03</td>
<td>0.80</td>
<td>0.11</td>
<td>0.10</td>
<td>0.18</td>
<td>0.08</td>
<td>0.13</td>
</tr>
<tr>
<td>Exper3</td>
<td>0.09</td>
<td>0.02</td>
<td>0.80</td>
<td>0.12</td>
<td>-0.01</td>
<td>0.14</td>
<td>0.06</td>
<td>0.12</td>
</tr>
<tr>
<td>Exper5</td>
<td>0.00</td>
<td>-0.02</td>
<td>0.81</td>
<td>0.21</td>
<td>0.10</td>
<td>0.19</td>
<td>0.10</td>
<td>0.16</td>
</tr>
<tr>
<td>Intent3</td>
<td>0.00</td>
<td>-0.13</td>
<td>0.26</td>
<td>0.77</td>
<td>0.28</td>
<td>0.33</td>
<td>0.40</td>
<td>0.37</td>
</tr>
<tr>
<td>Intent4</td>
<td>-0.16</td>
<td>-0.34</td>
<td>0.14</td>
<td>0.89</td>
<td>0.36</td>
<td>0.21</td>
<td>0.48</td>
<td>0.28</td>
</tr>
<tr>
<td>Intent5</td>
<td>-0.08</td>
<td>-0.32</td>
<td>0.16</td>
<td>0.87</td>
<td>0.30</td>
<td>0.25</td>
<td>0.47</td>
<td>0.28</td>
</tr>
<tr>
<td>Protec1</td>
<td>-0.25</td>
<td>-0.25</td>
<td>0.10</td>
<td>0.32</td>
<td>0.74</td>
<td>0.18</td>
<td>0.47</td>
<td>0.18</td>
</tr>
<tr>
<td>Protec2</td>
<td>-0.24</td>
<td>-0.17</td>
<td>0.06</td>
<td>0.29</td>
<td>0.80</td>
<td>0.20</td>
<td>0.42</td>
<td>0.20</td>
</tr>
<tr>
<td>Protec3</td>
<td>-0.11</td>
<td>-0.05</td>
<td>0.03</td>
<td>0.23</td>
<td>0.75</td>
<td>0.16</td>
<td>0.31</td>
<td>0.20</td>
</tr>
<tr>
<td>Protec4</td>
<td>-0.19</td>
<td>-0.14</td>
<td>0.08</td>
<td>0.30</td>
<td>0.77</td>
<td>0.15</td>
<td>0.34</td>
<td>0.13</td>
</tr>
<tr>
<td>Protec5</td>
<td>-0.12</td>
<td>-0.06</td>
<td>0.04</td>
<td>0.25</td>
<td>0.71</td>
<td>0.10</td>
<td>0.29</td>
<td>0.20</td>
</tr>
<tr>
<td>S_nor1</td>
<td>-0.10</td>
<td>-0.12</td>
<td>0.29</td>
<td>0.30</td>
<td>0.14</td>
<td>0.79</td>
<td>0.21</td>
<td>0.39</td>
</tr>
<tr>
<td>S_nor2</td>
<td>0.02</td>
<td>-0.12</td>
<td>0.15</td>
<td>0.27</td>
<td>0.20</td>
<td>0.85</td>
<td>0.11</td>
<td>0.43</td>
</tr>
<tr>
<td>S_nor3</td>
<td>-0.02</td>
<td>-0.08</td>
<td>0.17</td>
<td>0.23</td>
<td>0.18</td>
<td>0.85</td>
<td>0.13</td>
<td>0.40</td>
</tr>
<tr>
<td>S_nor4</td>
<td>-0.05</td>
<td>-0.05</td>
<td>0.18</td>
<td>0.23</td>
<td>0.18</td>
<td>0.78</td>
<td>0.14</td>
<td>0.38</td>
</tr>
<tr>
<td>Trus3</td>
<td>-0.19</td>
<td>-0.19</td>
<td>0.05</td>
<td>0.44</td>
<td>0.41</td>
<td>0.15</td>
<td>0.85</td>
<td>0.11</td>
</tr>
<tr>
<td>Trust2</td>
<td>-0.13</td>
<td>-0.11</td>
<td>0.11</td>
<td>0.40</td>
<td>0.35</td>
<td>0.16</td>
<td>0.71</td>
<td>0.15</td>
</tr>
<tr>
<td>Trust4</td>
<td>-0.22</td>
<td>-0.19</td>
<td>0.09</td>
<td>0.39</td>
<td>0.39</td>
<td>0.07</td>
<td>0.81</td>
<td>0.16</td>
</tr>
<tr>
<td>Trust5</td>
<td>-0.18</td>
<td>-0.17</td>
<td>0.08</td>
<td>0.39</td>
<td>0.42</td>
<td>0.17</td>
<td>0.75</td>
<td>0.17</td>
</tr>
<tr>
<td>Trust6</td>
<td>-0.19</td>
<td>-0.26</td>
<td>0.12</td>
<td>0.49</td>
<td>0.41</td>
<td>0.17</td>
<td>0.84</td>
<td>0.17</td>
</tr>
<tr>
<td>Use4</td>
<td>0.02</td>
<td>-0.04</td>
<td>0.19</td>
<td>0.34</td>
<td>0.18</td>
<td>0.42</td>
<td>0.19</td>
<td>0.85</td>
</tr>
<tr>
<td>Use5</td>
<td>0.08</td>
<td>-0.01</td>
<td>0.16</td>
<td>0.29</td>
<td>0.23</td>
<td>0.41</td>
<td>0.14</td>
<td>0.88</td>
</tr>
<tr>
<td>Use6</td>
<td>-0.01</td>
<td>-0.08</td>
<td>0.13</td>
<td>0.29</td>
<td>0.20</td>
<td>0.42</td>
<td>0.15</td>
<td>0.82</td>
</tr>
</tbody>
</table>
Table 6-16 Discriminant validity

<table>
<thead>
<tr>
<th>Item</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. E-privacy awareness</td>
<td>0.81</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. E-privacy risk concerns</td>
<td>0.27</td>
<td>0.83</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Prior e-services experience</td>
<td>0.05</td>
<td>-0.02</td>
<td>0.81</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Intention to use e-government services</td>
<td>-0.09</td>
<td>-0.31</td>
<td>0.22</td>
<td>0.84</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Perceived e-privacy protection</td>
<td>-0.25</td>
<td>-0.19</td>
<td>0.09</td>
<td>0.37</td>
<td>0.76</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Social norms</td>
<td>-0.05</td>
<td>-0.11</td>
<td>0.24</td>
<td>0.31</td>
<td>0.21</td>
<td>0.82</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Perceived trustworthiness of e-government services</td>
<td>-0.23</td>
<td>-0.24</td>
<td>0.11</td>
<td>0.53</td>
<td>0.50</td>
<td>0.18</td>
<td>0.80</td>
<td></td>
</tr>
<tr>
<td>8. Perceived usefulness of e-government services</td>
<td>0.04</td>
<td>-0.05</td>
<td>0.19</td>
<td>0.37</td>
<td>0.24</td>
<td>0.49</td>
<td>0.19</td>
<td>0.85</td>
</tr>
</tbody>
</table>

### 6.4. Test of the structural model

Once the measurement model was validated the structural model was then evaluated.

The model and associated hypotheses are shown in Figure 6.2. As discussed in Chapter 5, the structural model was examined using two criteria: its ability to explain the variance in the dependent variables and the significance of path coefficients. These two criteria were tested in this research as described in the first two parts of this section. Relationship strengths and total effect are also reported.
6.4.1. Variance explained

The first evaluation procedure was to determine whether the model has the ability to explain the variance in the dependent variables. Table 6.17 below lists the $R^2$ values for the dependent variables. Only 7% of the variance in e-privacy risk concerns was explained by e-privacy awareness. Perceived e-privacy protection, social norms, prior e-services experience, and e-privacy risk concerns explained 28% of the variance in perceived trustworthiness of e-government services. Also 26% of perceived usefulness of e-government services was explained by social norms, e-privacy risk concerns, perceived e-privacy protection, and perceived trustworthiness of e-government services. The model explained 36% of variability in the intention to use e-government services.
6.4.2. **Assessment of path coefficients**

The second criterion used to validate the structural model was significance of the path coefficients. It was assessed by evaluating the t-values of the proposed relationships. All of the proposed hypotheses specify direction of the proposed relationship so a one-tailed test could be used. The Smart PLS bootstrapping calculation technique was used to generate the t-values. Table 6.18 below lists the values for path coefficient, standard deviation, and t-value for each of the proposed relationships.

Table 6.18 below shows that t-values for seven of the paths were significant, but that the following paths were not significant:

- Social norms to perceived trustworthiness of e-government services;
- Prior e-services experience to perceived trustworthiness of e-government services;
- E-privacy risk concerns to perceived usefulness of e-government services;
- Perceived trustworthiness of e-government services to perceived usefulness of e-government services.
Table 6-18 Significance of path coefficients

<table>
<thead>
<tr>
<th>Path</th>
<th>Path coeff.</th>
<th>Std. dev.</th>
<th>t values</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1: Social norms → Perceived usefulness of e-government services</td>
<td>0.46</td>
<td>0.05</td>
<td>9.64***</td>
</tr>
<tr>
<td>H2: Social norms → Perceived trustworthiness of e-government services</td>
<td>0.05</td>
<td>0.05</td>
<td>1.09</td>
</tr>
<tr>
<td>H3: Prior e-service experience → Perceived trustworthiness of e-government services</td>
<td>0.06</td>
<td>0.05</td>
<td>1.23</td>
</tr>
<tr>
<td>H4: E-privacy risk concerns → Perceived usefulness of e-government services</td>
<td>0.04</td>
<td>0.05</td>
<td>0.87</td>
</tr>
<tr>
<td>H5: E-privacy risk concerns → Perceived trustworthiness of e-government services</td>
<td>-</td>
<td>0.14</td>
<td>3.11***</td>
</tr>
<tr>
<td>H6: Perceived e-privacy protection → Perceived usefulness of e-government services</td>
<td>0.12</td>
<td>0.05</td>
<td>2.58**</td>
</tr>
<tr>
<td>H7: Perceived e-privacy protection → Perceived trustworthiness of e-government services</td>
<td>0.46</td>
<td>0.04</td>
<td>10.47***</td>
</tr>
<tr>
<td>H8: E-privacy awareness → E-privacy risk concerns</td>
<td>0.27</td>
<td>0.05</td>
<td>5.41***</td>
</tr>
<tr>
<td>H9: Perceived trustworthiness of e-government services → Perceived usefulness of e-government services</td>
<td>0.05</td>
<td>0.06</td>
<td>0.97</td>
</tr>
<tr>
<td>H10: Perceived trustworthiness of e-government services → Intention to use e-government services</td>
<td>0.48</td>
<td>0.04</td>
<td>11.49***</td>
</tr>
<tr>
<td>H11: Perceived usefulness of e-government services → Intention to use e-government services</td>
<td>0.27</td>
<td>0.05</td>
<td>6.05***</td>
</tr>
</tbody>
</table>

**p <0.01
***p <0.001

6.5. Hypotheses testing

The research model has 11 hypotheses as shown in Figure 4.1. Figure 6.3 below summarises the results of the testing.
The results of the PLS model tests for each of the hypotheses are described below.

**Hypothesis H1:** Social norms will positively influence the level of perceived usefulness of e-government services.

Social norms demonstrated a significant positive influence on the level of perceived usefulness of e-government services. Therefore, this hypothesis was supported.

**Hypothesis H2:** Social norms will positively influence the level of perceived trustworthiness of e-government services.

Social norms did not demonstrate a significant influence on the level of perceived trustworthiness of e-government services. Therefore, this hypothesis was not supported.
Hypothesis H3: Prior e-services experience will positively influence the level of perceived trustworthiness of e-government services.

Prior e-services experience did not demonstrate a significant influence on perceived trustworthiness of e-government services. Therefore, this hypothesis was not supported.

Hypothesis H4: E-privacy risk concerns will negatively influence the perceived usefulness of e-government services.

E-privacy risk concerns had no significant influence on perceived usefulness of e-government services. Therefore, this hypothesis was not supported.

Hypothesis H5: E-privacy risk concerns will negatively influence the level of perceived trustworthiness of e-government services.

E-privacy risk concerns demonstrated a significant negative influence on the level of perceived trustworthiness of e-government services. Therefore, this hypothesis was supported.

Hypothesis H6: Perceived e-privacy protection will positively influence the level of perceived usefulness of e-government services.

Perceived e-privacy protection demonstrated significant positive influence on perceived usefulness of e-government services. Therefore, this hypothesis was supported.

Hypothesis H7: Perceived e-privacy protection will positively influence the level of perceived trustworthiness of e-government services.

Perceived e-privacy protection demonstrated significant positive influence on the level of perceived trustworthiness of e-government services. Therefore, this hypothesis was supported.
Hypothesis H8: E-privacy awareness will positively influence the level of e-privacy risk concerns.

E-privacy awareness significantly influenced the level of e-privacy risk concerns. Therefore, this hypothesis was supported.

Hypothesis H9: Perceived trustworthiness of e-government services will positively influence the level of perceived usefulness of e-government services.

Perceived trustworthiness of e-government services impact was not demonstrated to have a significant influence on perceived usefulness of e-government services. Therefore, this hypothesis was not supported.

Hypothesis H10: Perceived trustworthiness of e-government services will positively influence the intention to use e-government services.

Perceived trustworthiness of e-government services demonstrated a significant positive influence on the intention to use e-government services. Therefore, this hypothesis was supported.

Hypothesis H11: Perceived usefulness of e-government services will positively influence the intention to use e-government services.

Perceived usefulness demonstrated a significant positive influence on the intention to use e-government services. Therefore, this hypothesis was supported.
6.6. **Assessment of relationships strength**

The strength of the significant relationships was also of interest as mentioned in Chapter 5. Relationships were said to be weak if correlations were less than 0.2 and moderate in strength if between 0.2 and 0.5 and strong if more than 0.5 (Cohen, 1988). As can be seen in Figure 6.3 above, the analysis showed that there were no strong relationships.

The following relationships were of **moderate strength**:

- Social norms and perceived usefulness of e-government services;
- Perceived e-privacy protection and perceived trustworthiness of e-government services;
- E-privacy awareness and e-privacy risk concerns;
- Perceived trustworthiness of e-government services and intention to use e-government services;
- Perceived usefulness of e-government services and intention to use e-government services.

The following relationships were of **weak strength**:

- Perceived e-privacy protection and perceived usefulness of e-government services;
- Social norms and perceived trustworthiness of e-government services;
- E-privacy risk concerns and perceived usefulness of e-government services;
- E-privacy risk concerns and perceived trustworthiness of e-government services;
- Prior e-services experience and perceived trustworthiness of e-government services;
6.7. **Assessment of total effects**

Constructs within models influence one another directly and indirectly. Indirect relationships between two constructs are mediated by one or more intervening constructs. Therefore, in addition to the direct relationships shown in Table 6.18 and Figure 6.3, indirect relationships were also of interest. Table 6.19 below lists the total effects (both direct and indirect) estimated for the proposed model.

As can be seen, social norms and perceived e-privacy protection were the major influences on intention to use e-government services: social norms via its influence on the perceived usefulness of e-government services and perceived e-privacy protection via its influence on perceived trustworthiness of e-government services. The effect of social norms was three times as strong as that of perceived e-privacy protection.

E-privacy awareness and e-privacy risk concerns had limited influence on intention to use e-government services, and prior e-services experience played no role.

<table>
<thead>
<tr>
<th>Table 6-19 Total effects</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>Social norms</td>
</tr>
<tr>
<td>E-privacy awareness</td>
</tr>
<tr>
<td>E-privacy risk concerns</td>
</tr>
<tr>
<td>Prior e-services experience</td>
</tr>
<tr>
<td>Perceived e-privacy protection</td>
</tr>
</tbody>
</table>

*p <0.05       ***p <0.001
6.8. Participants’ extra feedback

The questionnaire included a section to collect the respondents’ extra written comments and feedback. The main points noted by respondents are summarized below.

**E-government awareness requirement**

Some respondents expressed their views regarding the importance of e-government awareness efforts for the Oman e-government project to succeed. They noted that awareness should include, but not be limited to, e-privacy awareness. Awareness as they saw it was a way to convince the citizen to use the new services. Some respondents believed that the government was not making sufficient efforts in this area. For example, one respondent commented “Government should run a comprehensive awareness plan and thereafter it should be left optional to the citizen to take an aware decision”. Some respondents however also thought that once there is sufficient awareness the citizens should be left to choose whether to use e-government services or not, and that use should not be imposed on citizens. For example one respondent commented “I think e-government should be gradually introduced to the citizen”. This issue was partially covered by the research as it examined e-privacy awareness and its role in e-privacy risk concerns.

**E-privacy protection necessity**

Several respondents thought that the e-government services project is a good idea for its usefulness however they fear its risks. They commented that the e-government services project should be strongly protected and e-privacy security should be ensured. For example, one responded commented “E-privacy should be granted and the systems should be protected”. Some respondents doubted that e-government services sites had
sufficiently secured environments as noted in the following comment: “it should be a secured environment but it is not”. Some respondents also noted the need for legislation to enhance the trustworthiness of e-government services. Yet others stated that e-government services were not yet popular in Oman and that they did not foresee the need for e-privacy concerns. The research model included this issue and its impact was examined.

**Weak infrastructure**

Several respondents thought that Oman’s ICT infrastructure is too weak to support a successful e-government project. They stated that the Internet speed in Oman was very slow and it could not support the project goal of having the citizens involved in adopting e-services: “the Internet speed should be increased for us to use e-services.” Another respondent stated “I would not use e-services using the existing dial-up.” This point is however outside of the scope of this study.

### 6.9. Summary

This chapter reported the results of the data analysis undertaken to test the proposed model. Firstly, the descriptive characteristics of the participants and their use of e-government at the time of the survey were presented. Very low levels of current use were reported. The chapter then presented the assessment of the measurement model. The final measurement model was satisfactory and hence suitable for testing the structural model. The chapter then presented the evaluation of the structural model against the criteria established in Chapter 5 and the results of the tests of the hypotheses were presented. This testing included the ability of the model to explain variance in the dependent variables and significance of path coefficients. Finally, respondents’ contributions to the questionnaire feedback section were also presented. Chapter 7
presents the results of the analysis of the interview data, which is used to compliment and triangulate the quantitative findings. Chapter 8 discusses the results that have been presented in this chapter and those from Chapter 7.
Chapter 7. Qualitative Findings

7.1. Introduction

As described in Chapter 5 this research involved both quantitative and qualitative analysis. The qualitative analysis was used to complement the quantitative findings. This chapter presents the results of the qualitative analysis as described in Chapter 5. Section 7.2 provides background information about the interview participants. The research model as presented in Chapter 4 consists of seven constructs that are proposed to impact the intention to use e-government services. The constructs were expected to influence the intention to use e-government services either directly or indirectly. Section 7.3 provides an analysis of comments made by the participants with respect to the constructs from the model. Section 7.4 examines whether the qualitative data obtained from the interviews is consistent with the research hypotheses as presented in Chapter 4. Each of the hypotheses is considered in turn. In Section 7.5 additional comments provided by the participants are discussed. The section highlights the participants’ perceptions of the success of the e-government services project in Oman. It also presents factors that the participants believe are needed for the project to succeed. The chapter concludes in Section 7.6 with a short comparison of the quantitative and qualitative findings.

7.2. Background information

As previously mentioned, 19 interviews were carried out as a part of the qualitative data collection process. All of the interviews were carried out at locations selected by the participants. The interviews were conducted in Arabic and were digitally recorded. Table 7.1 provides background about the participants and indicates the length of each interview.
As seen in the table above, 12 of the participants in the interviews were male (63.2%) and seven were female (36.8%). All participants had between three and 10 years computer experience and 58% rated themselves as having solid ICT skills (including Internet and e-services). The table also indicates that participants had a range of position titles which suggests that they have a variety of backgrounds in relation to ICT use.
Interview sessions took 28.13 minutes on average. The first column of the Table 7.1 lists each interviewee’s reference number (also used on each transcript). Throughout this chapter, and elsewhere, interview reference numbers are used to refer to each specific interview, and these are supplemented with the interview question number to identify the quotations used (e.g. 3:B4 refers to the third interviewee’s response to Part B Question 4 from the interview guide).

7.3. Qualitative findings relating to research constructs

The research model as presented in Chapter 4 consists of seven constructs that are proposed to impact the intention to use e-government services. The constructs were expected to influence the intention to use e-government services either directly or indirectly. This section provides an analysis of comments made by the interview participants with respect to the constructs from the research model and is based on the interview data as presented in Appendix E and F.

7.3.1. Prior e-services experience

Until relatively recently e-government services were not available in Oman. Although most of the participants had solid levels of ICT background (see Table 7.1), fewer had e-services experience, and even fewer said that they had used e-government services. Fifteen participants out of 19 had used e-services and the remaining four participants knew of some e-services but had not used them. For example, Interviewee 8 stated, “I have used the computer for 20 years. I did not use e-services much because I am worried as I know of many possible risks” (8: A2). Interviewee 16 also stated, “Yes but not e-government services” (16: A1). Some participants mentioned that at this stage of the implementation of e-government manual transactions were often faster. Interviewee 5 stated “in Oman at this stage manual transactions are faster” (5: B4).
Others mentioned that they used e-government services. For example, Interviewee 11 said, “Yes I did use some e-government sites such as the Central Bank, ROP, and other private sector sites” (11: A1). Interviewee 5 described his use of e-government services by “I have used e-services since 2002 and I used the government sites since 2005” (5: A1).

The most commonly known or used e-government services in Oman as mentioned by Interviewees were: e-schooling, Higher Education Registration site, Royal Oman Police online services (e-visa, traffic fines), Ministry of Manpower online services, e-tendering, Muscat Municipality online services, One Stop Shop, ITA site, Ministry of Interior for election services, Financial Security Market, Royal Hospital health records. E-commerce services that were mentioned by the interviewees as being used, or known of, included: hotel online reservations, online banking, Omantel site, IBM online services, and airline ticketing e-services.

7.3.2. Social norms

The majority of the participants (16) did not comment on the role of social norms in their future use of e-government services. Only two participants clearly stated that social norms would impact their future decisions. For example: “Family members and friends usually apply some pressure on my general decisions more specifically on using e-government services. They think e-services are not completely safe yet” (4: B4). Interviewee 3 was less confident of the role of social norms: “They might influence my decision only whenever I am ready to be convinced that such service is secured and it is of importance to me” (3: B4). One participant indicated that social norms would not influence their future decisions: “No one can influence my decision” (9: B4). It was
concluded that social norms may influence the decisions of some Omanis to use e-government services.

7.3.3. **E-privacy risk concerns**

Many participants did not know about possible e-privacy risk concerns, as using online services was still new and therefore there had been almost no incidents of e-privacy breaches. Interviewee 17 stated, “No one in Oman is talking about e-privacy” (17: B2). Interviewee 10 thought that a lot of people did not know about e-privacy risks and that was why they were not very concerned yet, however they were concerned about accessing their money online. He stated, “Because of lack of knowledge, a lot of people do not think it is of importance. People still worry about losing their online money” (10:C1).

Others were not sure about the meaning of e-privacy risk concerns and they thought that such concerns did not exist in Oman. One of those was Interviewee 9 who stated, “We hear and read about it. I think it is whenever someone abuses somebody’s e-privacy. I have heard about it elsewhere but not in Oman” (9:C1).

The lack of knowledge of e-privacy risk concerns in Oman was not only among ordinary citizens but also among educated and technical people. Interviewee 19 described the status by saying “Up to today a lot of educated people are not aware of online security risks, what about the ordinary citizen?” (19: B2). Interviewee 3 thought that e-privacy risk concerns not only threaten ordinary users but technical users too. He stated, “I have an excellent IT background and I worry about the e-privacy risks. What about the ordinary person?” (3: B2).
Some participants did show concerns about e-privacy risks. However, those interviewees who had e-privacy risk concerns varied in their understanding of the concerns. Interviewee 2 said “I think e-privacy risks might come from hackers who are able to abuse/ use our personal data with no permission” (2:C1). Interviewee 6 was concerned with “Misusing my personal data” (6:C1). Interviewee 7 further described his e-privacy risks concerns as:

“Unauthorized use of my personal data, such use might affect people financially or socially. Parents nowadays have to watch their children not only while they are out of the house but even when they are in the house with them. It is a disaster for IT illiterate parents. All online personal data concerns me as there is a chance for other people to abuse it. What concern me are my children, family, and financial data” (7:C1).

However, their fears may have been caused due to lack of knowledge and awareness. Interviewee 4 described his concerns as:

“Yes, I am concerned about somebody misusing my personal data. I am mostly concerned about somebody using my data for political or criminal misuse where I am innocent. Yes, people will not give their information if any risk is anticipated. They are also worried that the action wanted might be delayed due to such possible information abuse” (4:C2).

Interviewee 5 thought that although e-privacy risk concerns do exist among Omanis they should not deter people from using e-services. He stated:

“Concerns do exist. Privacy risks are there and we have to protect privacy as much as possible. The concerns should not be an obstacle. The Internet is like using airplanes. People used to worry that flying from one place to another will
spread and transmit viruses and diseases, but today who can live without flying sometimes?” (5:C1).

Interviewee 11 described his e-privacy concerns as

“My main concern is that my data might be used by a third party without any authorization. The concerns are always there as 100% protection does not exist” (11:C2).

Because some participants feared e-privacy risks they thought that avoiding the use of e-government services would help them in protecting their personal information. Interviewee 8 recommended this by stating “I do not advise anybody to put their personal data online” (8:C1). If views such as this spread among citizens they could become an obstacle to e-government project success because the citizens’ data is very necessary to e-government services systems as mentioned in Chapter 3.

Revisiting the participants’ responses above, it was clear that some participants did have concerns about their e-privacy. But some of them were not very aware of e-privacy risk concerns; and stated that they needed to know more about it. In general most participants thought that despite any concerns about e-privacy they would continue using e-government services. They perceived that the usefulness of these services outweighed the expected risks but they would keep their eyes open for any possible risks.

7.3.4. **Perceived e-privacy protection**

Interviewees mostly agreed on the importance of e-privacy protection. They said they would use e-government services sites if they feel that the sites are protected and
electronically secured. Interviewee 2 stated, “I will trust e-services whenever I feel they are protected. If not I will not give my personal data” (2:D2). Interviewee 16 also added, “I will always use e-government services whenever there are e-government sites that are secured. Security and awareness are needed to enhance e-government services use” (16:D2). Interviewee 13 confirmed the importance of e-privacy protection by saying,

“If the government gave me security guarantees, I would use it. ... the citizen is in need of the following to use e-services:

- Security guarantees
- Easy access
- Comprehensive content
- Awareness” (13:D2).

Interviewees 15, 16, and 19 recommended some additional e-privacy protection techniques for the government to put in place in order to get the citizens using e-government sites, these techniques can be summarized as follows:

- Online regulations;
- Authentication technology;
- Use of a third party who is qualified in information security in order to fully protect the privacy and security of data;
- Make efforts to increase awareness of e-privacy risks.

Although most of the interviewees thought that the government should have enough security measures to protect their online data, they still didn’t believe that sufficient security can be achieved.
Interviewee 11 noted, “I think that e-government sites should be secured as the government is responsible for all official information. I have heard about e-security solutions however I think none of them can do the job even within e-government sites” (11:C1).

Interviewee 13 added, “I believe that there is no possibility of full protection” (13:D2).

In regard to e-privacy protection, interviewees had variations in their own practices. Some people did not practice e-privacy protection measures. Some of them decided not to use e-services sites whenever their personal data was requested. Two of those were Interviewees 1 and 8.

Only six interviewees out of 19 stated that they had prior experience with protecting their e-privacy by practicing some e-privacy protection measures. Some of these had used known security measures such as periodic changing of online passwords, firewalls, cyber cards, and searching for online privacy policies.

Interviewee 5 said that he used firewalls. He described his e-privacy protection experience by saying, “I choose the well known sites. I use firewalls and I don’t use computers to store my personal data” (5: C8). Interviewee 7 used the cyber card technology. He said, “I only use the common protection technology, such as cyber cards with limited amounts” (7: C8).

Interviewee 13 stated that he searched for online policies before using the site and he described his actions by, “I do take precautionary actions when I deal with e-commerce
sites. I do not use sites if I doubt their security measures. I search for online privacy policies before using the site” (13: C8).

Several interviewees indicated that they had used other techniques such as giving incorrect information and storing data in computers that are not connected to the Internet. Interviewee 6 stated, “I take normal steps such as regular change of passwords. I also use false data whenever possible. Of course false data can not be used whenever dealing with the government” (6: C8). Interviewee 16 also said, “Sometimes I provide incorrect information” (16: C8).

7.3.5. E-privacy awareness

Almost all participants agreed that e-government awareness efforts in Oman were minimal and insufficient to promote the adoption of e-services. Interviewee 1 stated “Awareness efforts in Oman are very low and not sufficient” (1:B2). Interviewee 5 also described such insufficiency by saying “No, it is not adequate and not comprehensive. ITA should apply more awareness efforts and government information systems should be fully protected” (5:B2). Furthermore Interviewee 16 also indicated that awareness should include, but not be limited to, e-privacy awareness by saying, “No, there is not enough awareness. In order to get citizens to use e-government services awareness efforts should be increased” (16:B2). This is consistent with some unsolicited comments received with the questionnaire as discussed in Chapter 6.8.

Due to this lack of awareness some people wondered whether the e-government project had been executed yet, one of those was Interviewee 13 who said, “I don’t hear that there is an effective awareness effort. To find an excuse for the government, I try to convince myself that the project is not executed yet” (13:B2).
Some participants noted that e-government awareness efforts in Oman were not only not sufficient but very rarely covered online security in general and e-privacy security specifically. Some participants believed that ITA is mainly focussing on marketing the project and somehow neglecting the security awareness needs. This point was supported by Interviewee 3 who said, “ITA started a long time ago. Awareness isn’t comprehensive enough to cover privacy risks or to cover all places in the country” (3:B2). Interviewee 4 also said, “Awareness efforts are not adequate and not covering the security risks” (4:B2). Interviewee 6 added, “ITA is not talking about the risks and they are concentrating right now more on the promotion aspects. The government thinks that if they start talking about risks then they might stop people from using the services. I think such awareness should not be forgotten thus it should be gradually given to the people” (6:B2).

Interviewee 10 also stated, “Not enough e-privacy awareness. It is not comprehensive enough to cover online security” (10:B2).

Others thought that the awareness efforts were acceptable and that ITA will do what is needed at each phase of project execution. Among those was Interviewee 14 stating, “Awareness is OK despite that it is at its beginning” (14:B2). Interviewee 2 also stated, “Although ITA is making efforts that are appreciated, citizens are not made aware of e-government services possible risks” (2:B2).

Several interviewees suggested that ITA adopt some strategies in order to enhance the effectiveness of awareness efforts such as using the local media and e-services portals
themselves. Interviewee 7 indicated that the government should increase the awareness efforts by saying,

“The government is not making enough effort to make the citizens aware of online risks. Local classical media channels are not very effective nowadays, therefore, awareness should be through the service portal itself” (7:B2).

Interviewee 18 also added that e-privacy awareness was not sufficient and stated,

“There is not enough effort. Oman should utilize the TV as a tool to reach people. Omanis at this stage know only very little about the issue” (18:B2).

7.3.6. **Perceived usefulness of e-government services**

Participants differed in their views when describing the usefulness of e-government services. Some viewed e-government services as saving time and money, providing 24/7 government services, and unifying government units to have common goals. Interviewee 1 stated, “Yes, it is to save time cost, and efforts. It is 24/7 government services. Unify government units to have common goals” (1:B1). Interviewee 16 also stressed the expected usefulness of e-government services by stating “Of course it is essential to provide ease of access to government services and save time and effort. E-government is 24/7 government service” (16:B1). Interviewee 4 thought that e-government will be useful despite the anticipated risks, he stated “Yes it is important and essential despite all anticipated risks” (4:B1).

Some participants thought that e-government is essential for Oman due to Oman’s various geographical areas especially where the government has problems providing services via traditional means. Interviewee 6 stated,

“Yes it is very essential. Oman is a geographically difficult country and the
government is in need of such a medium to reach all of the citizens. It is needed for the citizens to use the government service easily and more efficiently” (6:B1).

Interviewee 7 believed that e-government services will be useful as a government-citizen interaction tool, but stressed the need for protection; he said “It enhances our daily interaction with the government. Thus the data should be highly protected from unauthorized use” (7: B1). Interviewee 19 also linked usefulness to information protection needs by stating “I expect e-government will help me utilize its usefulness but I will pay special attention to e-privacy risk” (19:D1). Many participants expected that e-government services would reduce manual work and would help Oman to go with global trends. Interviewee 11 stated, “E-government services will reduce manual work. It is also to keep up with the global trends and to have more governmental transparency” (11:B1).

The list below summarises the many benefits identified by the participants:

- More efficiency. This includes saving time, money, and effort;
- Reduce paper work;
- Better interaction;
- 24/7 access to government services;
- Greater geographical availability of government services;
- More government transparency;
- Unify government units to have common goals;
- Go with global trends;
- Reduce many other problems such as road traffic.
It seems that because of the benefits listed above most participants thought that the government should accelerate implementing the e-government services project. For example, Interviewee 1 said, “It saves the citizens time, efforts, and cost. However it has taken so long. The government should speed up the implementation process” (1:B3). Interviewee 14 also stated, “Nowadays, the infrastructure is weak, very few e-services are available, and no e-payment gateways. Therefore, the government should make it available to the citizens faster” (14:B3).

7.3.7. **Perceived trustworthiness of e-government services**

Many participants had a common view regarding the trustworthiness of e-government services in Oman. They believed that such services will be compulsory to use, and therefore issues of trust will be irrelevant. Interviewee 11 stated that he would trust e-government services because it is government; he described his view by saying,

> “If we have no option but to use it then we can not question the matter of trust. In general the citizen has no option but to give the data both manually and electronically. I will trust it as long as it is government related” (11:D1).

However, they thought that if the government allows use of e-government services to be voluntary, citizens would differ in their views regarding trustworthiness of e-government services. Interviewee 6 linked trustworthiness of e-government services to management factors; he stated,

> “If it is obligatory to use these services then the matter of trust can not be questioned. Otherwise it will depend on management and behavioural factors. The government related employees should be ethically controlled. All involved parties should have a high level of commitment” (6:D1).
Some participants believed that trusting the government is a default option as the
government already has most of their personal data and putting this data online will
make no difference. Such a view was supported by Interviewee 14 when he stated,

“Yes, it will be trusted as I automatically trust my government. However, those
working for it should have high ethics. When I fill in any application,
automatically, my authorization is given to the government to use my personal
data for any future transaction” (14:D1).

Others believed that if using such services is optional, they would trust e-government
services that meet certain requirements as listed below:

- The government should consult the citizens regularly in a partnership
  manner while implementing e-government services (Interviewee 4:D1);

- E-privacy trustworthiness has to be considered in relation to:
  o Ethics;
  o Culture and regulations;
  o Government transparency;
  o Maintaining a high level of commitment to delivering what has
    been promised;
  o Implementing e-law to increase e-government services
    trustworthiness (Interviewee 5:D1).

- The government should apply restricted access rights and strong system
  administration control. Interviewee 7 stated, “Those people who are not
  entitled to know my data should not know it, and those who should know it
  should know only what is required” (7:D1);
The government needs to have more e-privacy security assurance such as online policies, and comprehensive online regulations and e-laws (Interviewee 9:D1; Interviewee 13:D1);

Participants therefore were suggesting the following points for the government to act on in order to increase the citizens’ trust in e-government services:

- The government should come closer to the citizens and decide on e-government service in partnership with them;
- Enhance trust through effective awareness efforts;
- Provide online regulations and laws;
- Show a high level of commitment;
- People working on e-government need to increase their skills;
- Government related employees should follow ethical guidelines;
- Provide more e-privacy security assurance and online policies.

When comparing trustworthiness of e-government services to trustworthiness of e-commerce services, most participants thought that they would trust the government more highly just because it is government; as stated by Interviewee 11 “... I will trust it as long as it is government related” (11:D2). This point was supported by Interviewee 14 when he said, “...Yes, it will be trusted as I automatically trust my government. However, those working for it should have high ethics” (14:D1).

Moreover, Interviewee 13 said, “Yes, e-government is more trusted by the citizen” (13:C5). Others doubted e-government services trustworthiness, not because of bad government, but because not all government employees were perceived as trustworthy.
On the other hand some participants thought that they trusted e-commerce sites more than the governments’ as described by Interviewee 9 “.... _e-commerce sites are more trustworthy as they worry about their reputation, so the government should state that they worry in the same way_” (9:C4). Interviewee 10 did not trust e-government sites as she indicated “I do not think it is 100%. Government employees should respect people’s personal data. The citizens should know their rights and obligations” (10: D1).

Interviewee 14 supported this point by stating, “I automatically trust my government. However, those working for it should have high ethics” (14:D1). In contradiction, Interviewee 13 was one of those who did not trust either type of e-services site. He said, “Yes, e-government is more trusted by the citizen. However I think both are not trustworthy. E-commerce might think about their reputation more than they would think about me” (13:C5).

### 7.3.8. Intention to use e-government services

Despite the anticipated e-privacy risks concerns, most participants indicated that they would use e-government services whenever available. Interviewee 5: “I am going to use e-government services whenever they exist despite all concerns and risks” (5:D2).

Interviewee 3 also stated “I will use e-government. I am a gambler and risk taker as long as there are benefits expected” (3:D2). Interviewee 8 supported such a point by saying, “Despite any risk expectation, I will use it because I think it would be more efficient” (8:D2). Interviewee 17 added that he would use e-government services enthusiastically, “I am one of those who have a high level of enthusiasm. I am looking forward to using e-services for their usefulness despite any expected risks” (17:D2).

Others stated that they would use it despite some doubt, for example Interviewee 6 said, “I usually trust a thing until something wrong happens” (6:D2).
On the other hand, some other participants stated that they would use e-government services, not because they wanted to but because they thought that they would have to. For example, Interviewee 4 said, “I do not think the government will ask for my opinion. I will use it because I would have to” (4:D2).

Some participants further elaborated that they would not use it if it is left to their choice and they will find other ways to conduct their interactions with the government. Interviewee 19 also said, “Yes I will use it if I have no choice. I will not take chances if I don’t have to and I will think twice before taking any related decision” (19:D2). Interviewee 9 further added “We will have no other way but to use it. If e-services are voluntary I will try my best to find other ways” (9:D2). Interviewee 15 also stated that he will use e-government services because he would have no option but to use them. He described his point by saying, “I will use the service. The government already has my data” (15:D2). Others stated that they will use e-government services under certain conditions and will take precautions as indicated previously in this section.

7.4. Support for the research hypotheses

This section examines whether the qualitative data obtained from the interviews is consistent with the research hypotheses as listed in Chapter 4. The discussion of each hypothesis below is based on the interview data as presented in Appendix G.

*Hypothesis H.1 Social norms will positively influence the level of perceived usefulness of e-government services.*

As previously mentioned, not many participants commented on the impact of social norms. Several participants identified its importance, such as Interviewee 4 who stated,
“Family members and friends usually practice some pressure on my general decisions and using e-government services more specifically” (4:B4).

However, no one explicitly addressed the relationship between social norms and usefulness of e-government services. Therefore no conclusion has been drawn from the qualitative data about the role of social norms in influencing the perceived usefulness of e-government services.

_Hypothesis H.2 Social norms will positively influence the level of perceived trustworthiness of e-government services._

The interview data was not in agreement with this hypothesis. Interviewee 3 denied the influence of social norms on trustworthiness of e-government services by stating, “They might influence my decision only whenever I am ready to be convinced and persuaded that such service is secured and it is of importance to me” (3:B4). Interviewee 4 also thought that as the people of Oman were not yet using online transactions heavily, the impact of social norms on level of trustworthiness of e-government services was very limited. He said,

“Family members and friends ....think e-services are not completely safe yet. Citizens of Oman usually do not highly care for e-privacy, and not much personal information is online yet, so it would make little difference whether we use e-government services or not” (4:B4).

_Hypothesis H.3 Prior e-service experience will positively influence the level of perceived trustworthiness of e-government services._

Although most participants had good ICT experience not many of them had strong e-services experience. The interview data did not support the hypothesis. In fact some
responses indicated just the opposite influence. For example, Interviewee 3 stated, “I have an excellent IT background and I worry about the e-privacy risks.” (3: B2)

Hypothesis H.4 E-privacy risk concerns will negatively influence the level of perceived usefulness of e-government services.

The interview data is not consistent with this hypothesis. Most participants thought that they would use e-government services despite all possible risks. However there were some participants who believed that they might think twice before using the services. Interviewee 4 did not think concerns about e-privacy risks influenced perceived usefulness. He stated, “Yes it is important and essential despite all anticipated risks” (4:B1). Interviewee 19 stated that her perceptions of usefulness of e-government services will not be influenced by e-privacy concerns however she will keep her eyes open. She described her point of view by saying “I expect e-government will help me appreciate its usefulness but I will pay special attention to e-privacy risk” (19:D2).

Hypothesis H.5 E-privacy risk concerns will negatively influence the level of perceived trustworthiness of e-government services.

The interview data was strongly consistent with this hypothesis. Interviewee 4 said, “Yes, people will not trust the site if any risk is anticipated” (4:C2). Interviewee 1 also stated, “What always concerns me is that some sites are not trustworthy” (1:C2).

Hypothesis H.6 Perceived e-privacy protection will positively influence the level of perceived usefulness of e-government services.

The interview data was consistent with this hypothesis. For example Interviewee 13 thought that the lack of protection would decrease the usefulness of these services. He stated, “If the government gives me security guarantees, I would use it otherwise it
would be not very useful to me” (13:B4). Interviewee 7 also stated, “It is essential. government services are 24/7 and that enhances our daily interaction with the government. However the data should be highly protected from unauthorized use” (7:B1). Interviewee 11 said “If the citizen found that his data might be at a danger, negative reaction might be taken and he would avoid using it despite its expected usefulness” (11:B3).

Hypothesis H.7 Perceived e-privacy protection will positively influence the level of perceived trustworthiness of e-government services.

The interview data was strongly supportive of this hypothesis. Many participants were in agreement that e-privacy protection would increase the level of perceived trustworthiness of e-government services. Interviewee 2 said, “I will trust e-services whenever I feel they are protected, if not, I will not give my personal data” (2:D2). Similarly, Interviewee 5 indicated “Online law will increase the trustworthiness of e-government services” (5:C2). Interviewee 9 added, “To increase the trust the government needs to have more e-privacy security assurance, online policies, and the right regulations and laws” (9:C2). Interviewee 13 further agreed with the hypothesis by stating,

“If the government applies all protection efforts and it grants security, e-government services would be very trusted. However, if not it will not be trusted. The government should do all it takes to relax the citizens’ concerns and hurry up in having the online regulations and laws” (13:D1).

Hypothesis H.8 E-privacy awareness will positively influence the level of e-privacy risk concerns.

The interview data upheld this hypothesis. For example, Interviewee 6 stated that,
“talking about risks might stop people from using the services. I think such awareness should not be forgotten. It should be gradually given to the people” (6:B2).

**Hypothesis H.9** Perceived trustworthiness of e-government services will positively influence the level of perceived usefulness of e-government services.

The interview data was consistent with this hypothesis; for example, Interviewee 3 stated, “It would be of a greater usefulness if it is trustworthy. It will save me time, efforts, money however I would need to trust the site first” (3:D2). Interviewee 12 also stated, “Because I expect it to be trustworthy, I will enjoy the services usefulness and I will use Oman upper portal” (12:D2).

**Hypothesis H.10** Perceived trustworthiness of e-government services will positively influence the level of intention to use e-government services.

This hypothesis was strongly upheld by the interview data. Interviewee 16 said, “I will always use e-government sites that are secure” (16:D2). (1:B3). Interview 19 further agreed with the need for trust to use e-government services by indicating, “Yes, I will use it if I have no choice. I will not take chances if I don’t have to and I will think twice before taking any related decision” (19:D2).
Hypothesis H.11 Perceived usefulness of e-government services will positively influence the level of intention to use e-government services.

The interview data strongly supported this hypothesis. Interviewee 3 stated, “I will use e-government. I am a gambler and risk taker as long as there are benefits expected” (3:D2). Interviewee 8 also said “Despite any risk expectation, I will use it because I think it would be more efficient” (8: D2). Interviewee 17 further agreed and said, “I am one of those who have a high level of enthusiasm. I am looking forward to using e-services for their usefulness despite any expected risks” (17:D2).

Table 7.2 below summarizes the support provided by the qualitative analyses for the research hypotheses.
Table 7-2 Consistency of interview findings with hypotheses

<table>
<thead>
<tr>
<th>The hypothesis</th>
<th>Consistency of interview findings with hypothesis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypothesis H1: Social norms positively influences the level of perceived usefulness of e-government services</td>
<td>Not enough data to comment</td>
</tr>
<tr>
<td>Hypothesis H2: Social norms positively influences the level of perceived trustworthiness of e-government services</td>
<td>Not in agreement</td>
</tr>
<tr>
<td>Hypothesis H3: Prior e-services experiences positively influence the level of perceived trustworthiness of e-government services</td>
<td>Not in agreement</td>
</tr>
<tr>
<td>Hypothesis H4: e-privacy risk concerns negatively influences perceived usefulness of e-government services</td>
<td>Not in agreement</td>
</tr>
<tr>
<td>Hypothesis H5: E-privacy risk concerns negatively influence the level of perceived trustworthiness of e-government services</td>
<td>In agreement</td>
</tr>
<tr>
<td>Hypothesis H6: Perceived e-privacy protection positively influences the level of perceived usefulness of e-government services</td>
<td>In agreement</td>
</tr>
<tr>
<td>Hypothesis H7: Perceived e-privacy protection positively influences the level of perceived trustworthiness of e-government services</td>
<td>In agreement</td>
</tr>
<tr>
<td>Hypothesis H8: E-privacy awareness positively influences the level of e-privacy risk concerns</td>
<td>In agreement</td>
</tr>
<tr>
<td>Hypothesis H9: Perceived trustworthiness of e-government services positively influences the level of perceived usefulness of e-government services</td>
<td>In agreement</td>
</tr>
<tr>
<td>Hypothesis H10: Perceived trustworthiness of e-government services positively influences the level of intention to use e-government services</td>
<td>In agreement</td>
</tr>
<tr>
<td>Hypothesis H11: Perceived usefulness of e-government services positively influences the level of intention to use e-government services</td>
<td>In agreement</td>
</tr>
</tbody>
</table>
7.5. Participants’ perceptions of e-government services success in Oman

This section describes the findings related to the third type of the interview data (i.e. data not specifically related to the hypotheses) as mentioned in Chapter 5.7.2. The analysis of this data suggests that most participants believed that the e-government services project in Oman will be successful though it will take time. Most participants assumed that the e-government services project in Oman will take at least 5 years before it can be fully implemented.

Interviewee 4 stated, “Yes, sure it will succeed, but success will take time; it will take up to five years” (4:B3). Interviewee 14 said the project will need time in order to build up the required infrastructure and increase the number of e-government services, he said “Yes, it will but it will take 5-10 years.” (14:B3). Interviewee 5 also thought that the e-government services project will succeed in Oman because Oman is not the only country in the world implementing this sort of project. He thought that Oman should learn from others to avoid failure. He described his view by saying “Yes, Oman is not the only country implementing such projects. To avoid the factors that lead to failure, Oman should learn from others” (5:B3). Interviewee 15 supported the five year period for the project to succeed, by noting “Not in the near future and it will take not less than 5 years” (15:B3).

Some other participants thought that the e-government services project will gradually build up to implementation success and that such success might not be 100% as hoped. Interviewee 12 noted, “It will be, but gradually” (12:B3). Interviewee 6 also described the project’s success by saying, “Yes it will be successful, if not in full it will be in part. Things usually take time for the people to acknowledge the change” (6:B3).
Some participants proposed some key factors for the government to address in order to achieve its success goal. Interviewee 18 described e-government success by stating, “It is possible within 3-5 years and it will not be 100%. The main obstacles are weak infrastructure and access affordability. The digital divide between those who understand the use of IT and those who do not is still wide” (18:B3). As suggested by Interviewee 18, the e-government project in Oman should resolve some issues for it to succeed. These issues were weak infrastructure, access affordability, and the digital divide. Interviewee 16 believed that for the project to succeed it needs to reach the people and therefore awareness efforts should be increased. She stated, “Whenever there are sincere efforts the project will be successful. To reach the people, the project is in need of a lot of awareness” (16:B3). Interviewee 10 added that Oman should work on the digital divide and encourage innovativeness amongst school students in order to achieve the optimum e-government success. She made her point by saying, “In Oman the IT digital divide is not yet treated enough. The government should support students at schools to be more creative in the field of IT” (10:D2).

Other participants added some more suggestions on how to speed up the success of the project. Interviewee 10 suggested that the Omani government should make more sincere efforts to increase the cooperation across government units in the implementation of e-government services. She expressed her suggestions by saying, “We expect success as long as the efforts are sincere. Further cooperation between government units will increase the chances of success” (10: B3).

Interviewee 11 added, “E-government services success depends on the society’s awareness and readiness. The more people that use it successfully the more success
there will be” (11:B3). Interviewee 5 also thought that, “The human factor is the main obstacle; the government should encourage the younger citizens while promoting such projects” (5: B3). Interviewee 19 believed that the people in Oman could themselves be an obstacle if not ready and encouraged by the government to adopt the new services. She described her point by saying, “The main obstacles are the people’s mentalities, poor infrastructure, and limited awareness” (19:B3).

These key success issues to be addressed by the Omani government in order for the e-government services project to succeed can be summarized as follows:

- Better ICT Infrastructure;
- Effective awareness and project marketing and promotion;
- Narrowing the digital divide;
- Educating citizens especially adolescents and students;
- Cross government unit collaboration and cooperation;
- Executing relevant e-laws;
- Providing effective e-payment gateways.

On the other hand, some participants believed that it was too early to judge the e-government services project’s likelihood of success. Among those was Interviewee 9 who stated “It is too early to judge as I am away from the project. Yes it is slow but it is due to low demand. People will use it further as they get its benefits” (9:B3).

Interviewee 3 thought that e-government information services will succeed faster than the transactional services. He stated that
“The e-government informative services will succeed, however, transactional services will take longer as they will be faced with the integration and standardization requirements for all stakeholders” (3:B3).

7.6. Quantitative and qualitative findings

This section reflects the triangulation method that was chosen for this study as described in Chapter 5.2. As previously mentioned, the qualitative data was intended to complement the questionnaire findings and provide in-depth details of e-privacy risk concerns and their impact on citizens’ intentions to use e-government services. Both quantitative and qualitative approaches were used in a complementary manner to minimize the disadvantages of a single research method. This section compares the findings of the two approaches to draw out the overall research findings. As previously stated in Chapter 6.5, the analysis of the quantitative findings provided support for seven of the 11 hypotheses. Table 7.3 lists the proposed hypotheses and indicates whether the results from the qualitative analysis are consistent with them. The interview data is consistent with the quantitative findings for nine of the hypotheses. That is, six hypotheses that were supported by the quantitative analysis also found support from the qualitative analysis. Three hypotheses that were not supported by the quantitative analysis, also did not receive support from the qualitative analysis. There was insufficient data from the interviews to draw any conclusion about one of the hypotheses, and conflicting results were obtained for one hypothesis.
Table 7-3 Consistency between results of quantitative and qualitative analyses

<table>
<thead>
<tr>
<th>The hypothesis</th>
<th>Quantitative analysis</th>
<th>Is qualitative analysis consistent with quantitative analysis?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypothesis H1: Social norms positively influences the level of perceived usefulness of e-government services</td>
<td>Supported</td>
<td>Not sufficient evidence to say</td>
</tr>
<tr>
<td>Hypothesis H2: Social norms positively influences the level of perceived trustworthiness of e-government services</td>
<td>Not supported</td>
<td>Yes</td>
</tr>
<tr>
<td>Hypothesis H3: Prior e-services experiences positively influence the level of perceived trustworthiness of e-government services</td>
<td>Not Supported</td>
<td>Yes</td>
</tr>
<tr>
<td>Hypothesis H4: E-privacy risk concerns negatively influence perceived usefulness of e-government services</td>
<td>Not supported</td>
<td>Yes</td>
</tr>
<tr>
<td>Hypothesis H5: E-privacy risk concerns negatively influence the level of perceived trustworthiness of e-government services</td>
<td>Supported</td>
<td>Yes</td>
</tr>
<tr>
<td>Hypothesis H6: Perceived e-privacy protection positively influences the level of perceived usefulness of e-government services</td>
<td>Supported</td>
<td>Yes</td>
</tr>
<tr>
<td>Hypothesis H7: Perceived e-privacy protection positively influences the level of perceived trustworthiness of e-government services</td>
<td>Supported</td>
<td>Yes</td>
</tr>
<tr>
<td>Hypothesis H8: E-privacy awareness positively influences the level of e-privacy risk concerns</td>
<td>Supported</td>
<td>Yes</td>
</tr>
<tr>
<td>Hypothesis H9: Perceived trustworthiness of e-government services positively influences the level of perceived usefulness of e-government services</td>
<td>Not supported</td>
<td>No</td>
</tr>
<tr>
<td>Hypothesis H10: Perceived trustworthiness of e-government services positively influences the level of intention to use e-government services</td>
<td>Supported</td>
<td>Yes</td>
</tr>
<tr>
<td>Hypothesis H11: Perceived usefulness of e-government services positively influences the level of intention to use e-government services</td>
<td>Supported</td>
<td>Yes</td>
</tr>
</tbody>
</table>
7.7. **Summary**

This chapter discussed the findings from the qualitative phase of this research. The qualitative data analysis was undertaken to compliment the quantitative findings. The chapter first presented background information about the interview participants. The interviewees had range of different backgrounds in relation to ICT use, but over half of them rated themselves as having solid ICT skills. The next section of the chapter presented a construct by construct synthesis of the comments made by the participants with respect to the constructs from the research model. This was followed by an examination of whether the qualitative data obtained from the interviews is consistent with the research hypotheses. Each of the hypotheses was considered in turn. In most cases the qualitative data was consistent with the proposed hypotheses. Additional comments from the participants about likelihood of success of e-government services project in Oman were also presented. Most participants believed that the e-government services project in Oman will be successful though noted that it will take time.

Participants identified factors that they believe need to be addressed for the project to be successful. The chapter concludes with a brief comparison of the quantitative and the qualitative findings. It was found that the there was mostly agreement between the findings obtained using the different methodological approaches.

Chapter 8 presents a detailed discussion of both the quantitative and qualitative results and concludes the research study.
Chapter 8. Discussion and Conclusion

8.1. Introduction

This chapter discusses the quantitative and qualitative research results as presented in Chapters 6 and 7. Section 8.2 discusses the research model and the role of each construct in influencing the intention to use e-government services. In Section 8.3 the progress towards answering the two main research questions is discussed. The chapter then presents in Section 8.4 some limitations of the research and discusses the implications of the research and suggested future research. Some recommendations for practice to the Omani government are presented in Section 8.5. Section 8.6 concludes the thesis by summarizing the key features of the research and its significance.

8.2. Model discussion

The study reported on in this thesis examines the impact of e-privacy risk concerns on citizens’ acceptance of e-government services in Oman. It also considers the impact of users’ perceptions of e-privacy protection and their perceptions of the trustworthiness of e-government services, given their e-privacy risk concerns. This research introduced and tested a model of the role of online privacy in the adoption of e-government services. The model uses Liu et al.’s (2004) privacy-trust-behavioral intention model as a starting point. It also draws on the broader technology acceptance literature and recent work on e-privacy awareness and protection. The level of e-government services use in Oman was low at the time the research was undertaken as services are only slowly being introduced. Therefore the research uses intention to use as a surrogate for actual use.
Figure 8.1 below shows the supported paths for the model as found in this study. It shows that perceived usefulness of e-government services was influenced by social norms and perceived e-privacy protection. In turn, perceived usefulness significantly influenced the intention to use e-government services. The results therefore suggest that when citizens believe that the services are of value they are more likely to use them. Perceived trustworthiness of e-government services was also found to play an important role. It was influenced by citizens’ concerns about risk and perceptions of e-privacy protection, and in turn influenced the intention to use e-government services.

The model explained 35.8% of the total variance in the citizens’ intended adoption behavior. This is consistent with previous TAM related studies such as Bhattacherjee (2000) in which their model explained 41% of the variability in the intention to use electronic brokerages. Similarly, Ahn, Park and Lee’s. (2004) model explained 30.8% in the variability of the intention to purchase online, and Featherman and Pavlou’s (2003) model accounted for 36.6% of the variability in intention to adopt e-services. However the model’s overall explanatory power could possibly be increased by further
examining other factors such as some of those mentioned in Section 3.5. These include ease of use, facilitating conditions (Venkatesh et al., 2003) and culture (power distance acceptance and uncertainty avoidance) (Warkentin et al., 2002). This should provide a better understanding of citizens’ intentions to use e-government services.

The following sections discuss the model relationships and highlight the roles of each of the proposed factors in influencing the intention to use e-government services.

8.2.1. **Role of social norms**

As proposed, and consistent with TAM2 and previous research such as Horst et al. (2007) and Kim et al. (2009), social norms play a significant role in influencing citizens’ perceptions of the usefulness of e-government services. Social norms also indirectly impact the intention to use e-government services via perceived usefulness of e-government services. This study found that Omanis are no different from other adopters of e-services in that their perceptions of the usefulness of e-government services were influenced by whether people who are important to them want them to use e-government services.

As indicated in the interview data, many Omani people believe that the use of e-government services will become mandatory. For example, Interviewee 4 said, “I do not think the government will ask for my opinion. I will use it because I would have to” (4:D2). Interviewee 9 further added, “We will have no other way but to use it.” (9:D2). This finding therefore also supports the findings of Venkatesh and Davis (2000) and Lee et al. (2006) that the impact of social norms is more important when the use of the technology or services is perceived to be mandatory.
This study found that social norms did not influence the perceived trustworthiness of e-government services. Bolton et al. (2004) argued that although social norms is not the main factor influencing the perceived trustworthiness of a service it plays a role and Li et al. (2006) found that social norms do influence trusting attitude, trusting beliefs, and trusting intention to use information systems in the e-commerce domain. This study’s findings are therefore inconsistent with the literature from the e-commerce domain. There has however been no research so far on this relationship in the e-government domain. It appears that trustworthiness of e-government services may have different influences than trustworthiness of e-commerce services does.

The qualitative analysis suggested that the citizens assume that the government (and hence e-government services) is already trustworthy and hence are not influenced by others. For example, as stated by Interviewee 14, “Yes, it will be trusted as I automatically trust my government” (14:D1). However, this explanation did not receive support from the questionnaire data, as there was a wide range of perceptions of trustworthiness of e-government services (see Table 6-10). Possible reasons for this difference are discussed in Section 8.2.6.

The qualitative analysis also suggested that the lack of relationship could also be due to citizens’ assumptions that using the services would be mandatory. Interviewee 11 stated, “In general the citizen has no option but to give the data both manually and electronically.” (11:D1). As previously mentioned in Section 4.4, there is limited existing research on the relationship between social norms and the level of trustworthiness of e-government services; therefore it is highly recommended that future research should further clarify this relationship.
8.2.2. **Role of prior e-services experience**

Contrary to expectations, prior e-services experience did not influence the perceived trustworthiness of e-government services. This result is inconsistent with the results of studies such as Warkentin et al. (2002), Metzger (2004) and Nath (2005) that found that the more prior e-services experience users had, the more trust they had in e-services. The studies by Metzger (2004) and Nath (2005) were undertaken in the e-commerce domain and the unexpected findings could be related to the different domain. While Warkentin et al.’s finding was in the government domain they only tested one e-government system, a judicial system which was possibly not representative of other types of e-government services. Testing one very specialized system may not be enough to identify the relationships in the e-government services domain as these relationships might vary depending on particular type of e-government system. Examining a range of systems can help resolve this issue (Lee & Rao, 2005).

The lack of a relationship could also be due to the fact that the use of e-government services is relatively new in Oman; it may be that experience levels were too low to be able to detect an effect. However, the interview data suggested that even if users have considerable prior familiarity with the Internet and e-services usage, their confidence in these services was not likely to be influenced. For example, Interviewee 3 stated, “I have an excellent IT background and I worry about the e-privacy risks” (3: B2). Further research is recommended to have better understanding of this relationship.

8.2.3. **Role of e-privacy risk concerns**

The model proposed that e-privacy risk concerns negatively influence both the perceived usefulness of e-government services and the perceived trustworthiness of e-government services and through them indirectly impact the intention to use
e-government services. E-privacy risk concerns were found to influence the perceived trustworthiness of e-government services but not the perceived usefulness of e-government services. That is, citizens with higher levels of concerns had less trust in e-government services, but their opinions about usefulness were not influenced. This finding is very clear in the interview data. For example, Interviewee 4 stated “Yes it is important and essential despite all anticipated risks” (4:B1). Interviewee 6 also said, “I expect e-government will help me appreciate its usefulness but I will pay special attention to e-privacy risk” (19:D2). The findings also reflect the fact that Omanis as mainly typical Muslims worry about their family privacy rather than about other personal details (Reilly & Cullen, 2007). For example, Interviewee 7 said, “What concerns me are my children, family, and financial data” (7:C1).

The results related to the influence of e-privacy risk concerns on the perceived usefulness of e-government services are inconsistent with those of Featherman and Pavlou (2003) in the e-commerce domain who found that the more risks that users perceive, the less they believe that e-services are useful. Horst et al. (2007) had mixed findings with respect to the influence of e-privacy risk concerns on the perceived usefulness of e-government services. It was found to have an influence in one of the two samples they considered, but not the other. Lee et al. (2001) differentiated between perceived risks of services and perceived risks of products, and found that perceived risks of e-services had an influence on trustworthiness, but that perceived risks of products did not. The relationships associated with perceptions of risk are obviously complex and in order to better understand them it is recommended that future research on it is carried out.
The influence of e-privacy risk concerns on trustworthiness of e-services is consistent with Liu et al. (2004), Metzger (2004) and Suh and Hans’ (2003) findings in the e-commerce domain. Therefore the influence of e-privacy risk concerns on trustworthiness of e-government services is consistent with models of online exchange, including Jarvenpaa and Tractinsky’s Internet Consumer Trust Model (1999). This result is also consistent with Horst et al. (2007) and Reilly and Cullen (2007) in the e-government domain. Given the importance of e-privacy risk concerns and the influence they have on citizens’ perceptions of the trustworthiness of e-government services, governments should take action in order to increase the level of citizens’ confidence in e-government services.

8.2.4. Role of perceived e-privacy protection

As proposed in the model, perceived e-privacy protection influenced both perceived usefulness of e-government services and perceived trustworthiness of e-government services. Perceived e-privacy protection also indirectly impacted on the intention to use e-government services via perceived usefulness and perceived trustworthiness of e-government services. When citizens believe that e-government services sites are protected they are more likely to trust these services and perceive them as more useful, and then are more likely to use them. This is summarized by the following comment from Interviewee 13, “If the government gives me security guarantees, I would use it otherwise it would be not very useful to me” (13:B4).

These results are consistent with the findings of Horst et al. (2007) and Loukides and Shao (2007) with respect to perceived usefulness of e-services, and those of Carter and Bélanger (2005), Lee et al. (2003), Nath (2005) and Suh and Han (2003) with respect to perceived trustworthiness.
It was interesting to note that perceived e-privacy protection had a much stronger influence on perceived trustworthiness than it did on perceived usefulness of e-government services. Therefore attempts to keep e-privacy protected and secured, can not only increase citizens’ levels of trustworthiness of the e-government services but can also increase the expected usefulness of these services.

**8.2.5. Role of e-privacy awareness**

As proposed, e-privacy awareness significantly influenced e-privacy risk concerns. The more aware that citizens were of e-privacy issues, the more concerns they had. This result is consistent with that of Olivero and Lunt (2004) who explored a direct relationship between e-privacy awareness and e-privacy risk concerns in the e-commerce environment. It also supports the findings of Solaru (2005), Dinev and Hart (2006a) and Mahotra et al. (2004) that risk awareness (including e-privacy awareness) increases users e-privacy risk concerns indirectly.

E-privacy awareness also indirectly impacted on the intention to use e-government services via e-privacy risk concerns. The more that the citizens were aware of e-privacy risks, the more concerns they had and the less trust they had in these services, and the less willing they were to use them. This is consistent with the findings of Olivero and Lunt (2004) and Malhotra (2004) that risk awareness is a major factor that indirectly reduces the level of trust and in turn decreases the intention to use the services.

The interview participants in this study believed that the government should make the citizens gradually aware about e-privacy issues and ways of protection at the same time as it is marketing e-government services. Although this may increase the citizens risk
concerns it would assist the citizens to choose and to be more knowledgeable. For example, Interviewee 6 indicated “talking about risks might stop people from using the services. I think such awareness should not be forgotten. It should be gradually given to the people” (6:B2). This suggests that gradually increasing citizens’ awareness could result in them taking steps to improve protection. This possibility, and its role in increasing trust in e-government services, should be explored in future research.

8.2.6. Role of perceived trustworthiness of e-government services

The model proposed that perceived trustworthiness of e-government services influences the intention to use e-government services both directly and indirectly via perceived usefulness of e-government services. As proposed, perceived trustworthiness of e-government services was found to have a significant direct influence on the intention to use e-government services, however it did not have an influence on perceived usefulness of e-government services which suggests there was no indirect relationship between perceived trustworthiness of e-government services and the intention to use e-government services in this study.

The direct relationship is consistent with Malhotra et al. (2004), Belanger et al. (2002), and Liu et al. (2004) in the e-commerce domain. However, the result related to the relationship of perceived trustworthiness of e-government services to perceived usefulness of e-government services was not as expected. The findings are inconsistent with those of Horst et al. (2007), Lee and Rao (2005) and Pavlou (2003). This could be due to cultural differences in the participants, as emphasized by Warkentin et al. (2002), as none of the studies used to justify the hypothesis were conducted in Middle East countries. It could also be due to the early stage of usage of e-government services in Oman. Because citizens’ have had few negative experiences and possibly not been
made aware of negative experiences others have had, the potential relationship between trustworthiness and usefulness may not have been activated.

It is also possible that relationships within the e-government domain may differ from those in the e-commerce domain. In the e-commerce domain users normally have a choice of service providers, and hence have the ability to switch providers in situations where they lack trust or perceive that services are less useful. In the e-government domain, citizens do not have this flexibility, thus it seems likely that a service may still be perceived as useful, despite a lack of trust (there being potentially no other way to obtain conduct a transaction).

It was also interesting to note that the qualitative analysis did support the existence of a relationship between perceived trustworthiness of e-government services and perceived usefulness of e-government services. For example, Interviewee 12 said, “Because I expect it to be trustworthy, I will enjoy the services usefulness and I will use Oman upper portal” (12:D2). It is possible that the people who agreed to participate in an interview were more trusting people with more interest in the e-government implementation, and actually had fewer concerns about what could go wrong. It could also be possible that participants felt more constrained in the interview situation and were thus less able to express perceptions about possible lack of trustworthiness of e-government services, than were respondents to the anonymous questionnaire. As Table 6.10 shows, the perceptions of trustworthiness of e-government services in Oman varied greatly across the questionnaire respondents. Further research is required to understand this relationship.
8.2.7. **Role of perceived usefulness of e-government services**

Both the quantitative and qualitative results of this study supported the proposed relationship between perceived usefulness of e-government services and the intention to use e-government services. In other words, the more citizens perceive e-government services to be useful, the more they intend to use them. The finding is consistent with TAM2 and is also consistent with many other studies in the e-commerce domain such as Pavlou (2003) and Ahn et al. (2004). It is also consistent with several studies in the e-government domain such as Horst et al. (2007) and Lee and Rao (2005).

It was interesting to note, however, that the influence of perceived usefulness of e-government services on intention to use e-government services was only about half as strong as that of perceived trustworthiness. Whilst the intentions of the citizens of Oman to use e-government services are influenced by how useful they believe these services are, the trustworthiness of the services appears to be an even more important issue to them.

8.3. **Answering the research questions**

Chapters 1 and Chapter 4 stated the research questions to be answered in this thesis. This section discusses the progress of the study towards answering the research questions in order to meet the objectives of the research.

The primary objective of the research described in this thesis is to examine the impact of online privacy concerns on citizens’ acceptance of e-government services. It also considers what other factors impact on citizens’ intentions to use e-government services, such as information protection and the citizens’ ability to trust e-government
services, given their privacy concerns. The answers for the two research questions inclusively met the requirements of these objectives.

The first research question of the thesis was:

Q1. Do e-privacy risk concerns influence citizens’ intentions to use e-government services in Oman?

E-privacy risks have been considered to be an increasingly important hazard associated with using e-government services (Ackerman & Mainwaring, 2005; Belanger & Carter, 2008; Lau, 2003; Srivastava & Teo, 2005; Warkentin et al., 2002). Therefore, citizens’ e-privacy risk concerns were considered a potential obstacle to successful e-government services implementation.

The answer to this research question is that e-privacy risk concerns have a weak influence on the intention to use e-government service through perceived trustworthiness of e-government services. This means that the more e-privacy risk concerns that citizens have, the less trustworthy they perceive e-government services to be, and the less likely they are to intend to use e-government services. It was proposed that e-privacy risk concerns would also influence intention to use e-government services via an impact on the perceived usefulness of these services, but this was found not to be the case.

The second research question of the thesis was:

Q2. What other factors related to e-privacy influence citizens’ intentions to use e-government services in Oman?
The additional factors investigated were perceived e-privacy protection, social norms, prior e-services experience and e-privacy awareness. It was found that perceived e-privacy protection, social norms and perceived e-privacy awareness all influenced the citizens’ intention to use e-government services. Whereas perceived e-privacy protection influenced intention through both perceived trustworthiness of e-government services and perceived usefulness of e-government services; social norms had its influence only through perceived usefulness of e-government services.

The results also showed that e-privacy awareness significantly influenced the intention to use e-government services via its influence on e-privacy risk concerns. Thus the more a citizen knows about e-privacy risks the more concerned they become. This leads to reductions in the perceived trustworthiness of the services and hence a reduced intention to use e-government services.

The study did not however find that prior e-services experience influenced intention to use e-government services. This result suggests that no matter how much prior e-service experience citizens might have, their intention to use e-government services would not be affected. However, as citizens gain more specific e-government services experience this could change.

Perceived e-privacy protection was found to be the factor that had the most influence on intention to use e-government services and social norms had the second strongest influence. The influences of e-privacy awareness and e-privacy risk concerns were very weak.
8.4. Research limitations and research implications

This study did not face many significant obstacles; in fact, the research preparation and data collection process were fairly smoothly accomplished. The government employees in Oman were very cooperative. The research therefore was done as planned and in a timely manner and resulted in many implications for future practice and investigation. The following two sections discuss the main research limitations and the research implications.

8.4.1. The research limitations

There were two limitations of the study that need to be considered. The first is that the study took place during the early stages of e-government implementation in Oman. This early stage of implementation meant that intention to use e-government services was used as a surrogate for actual use. Therefore another study during the next 5 years would be of great value as more e-government services are expected to be in place.

The second possible weakness is that the participants in the study were limited to government employees. Government employees were chosen as participants because of the large proportion of the workforce they form, and because support was provided for the study by the government because of their commitment to ensuring successful uptake of e-government. It was interesting to note some differences between results obtained from the anonymous survey and from the interviews. It appeared that respondents to the questionnaire felt free to give their views about the trustworthiness of e-government services, but that those interviewed face to face may have been less free to do so. It is possible that participants felt more constrained in the interview situation and were thus less able to express perceptions about possible lack of trustworthiness of e-government services, than were respondents to the anonymous questionnaire. This indicated the
value of using the two complementary approaches in this study. Nevertheless it would be valuable to repeat the study with a broader sample.

8.4.2. The research implications

This study examined the role of e-privacy concerns in influencing citizens’ intentions to use e-government services. The study has highlighted the influence of several factors on the level of trust that citizens have in e-government services, and it has shown how perceived trustworthiness and perceived usefulness of e-government services influence citizens’ intentions to use e-government services. Whilst perceived usefulness of e-government services is important, perceived trustworthiness of e-government services was found to play a more important role in citizens’ intentions to use e-government services.

This research explored whether a direct relationship exists between social norms and perceived trustworthiness of e-government services. This relationship has not previously been tested in the e-government domain. The finding that there was not a relationship between social norms and perceived trustworthiness of e-government services could be considered an important contribution to the knowledge base by adding further understanding of this relationship in relation to e-government services adoption models.

Several of the findings are inconsistent with existing research. It would be valuable for future research to address issues such as the lack of influence of social norms on the perceived trustworthiness of e-government services and the lack of influence of e-privacy risk concerns on perceived usefulness of e-government services. Inconsistency in the findings of previous research on the impact of perceived
trustworthiness of e-services on the perceived usefulness of the service has already been noted in the existing research, with Horst et al. (2007) and Cullen and Reilly (2007) demonstrating the relationship, and Lee and Rao (2005) proposing that the relationship is in the opposite direction and showing that perceived usefulness influences perceived trustworthiness. Therefore this is another area that requires further examination in order to better understand how these relationships work in the e-government environment.

The study has made a contribution to scholarly knowledge by providing a more comprehensive model of e-government use and adoption. The research model was built based on previously developed models and extended them by introducing additional constructs and relationships that made it theoretically unique. Future research might build on the model. For example, the model’s explanatory power could possibly be increased by further examining the role of other factors such as some of those mentioned in Section 3.5. These include ease of use, facilitating conditions (Venkatesh et al., 2003) and culture (power distance acceptance and uncertainty avoidance) (Warkentin et al., 2002). This should provide a better understanding of citizens’ intentions to use e-government services.

This study is also considered to be the first of its type in Oman. This research focused on citizens concerns about the use of e-government services in Oman. Whilst it is true that there have been many studies elsewhere that have analyzed e-privacy impacts on acceptance of various Internet applications, this research has been predominately conducted in Western countries. There is almost no research that has specifically tackled such issues in Oman or nearby countries before. Therefore the research described in this thesis makes a valuable addition to e-government research.
The sampling frame for this study was the civil services government employees sector which forms approximately 20% of all manpower in Oman. Therefore this sample is quite representative of the Omani citizens, and differs from some studies where a small number of people such as those attending a community concert or a college were used as samples (e.g. Lee and Rao (2005)) and those studies that used small focus groups such as Cullen and Reilly (2007), and Carter and Belanger (2005). The sampling frame of this research therefore provided the research with an excellent opportunity to obtain the perceptions of a wider community and to provide more realistic implications for practice.

8.5. Recommendations for the Omani government

As previously discussed the study has highlighted the influence of several factors on the level of trust that citizens have in e-government services, and it has shown how perceived trustworthiness of e-government services and perceived usefulness of e-government services influence citizens’ intentions to use e-government services. The results suggest that the government should be sensitive to citizens’ e-privacy concerns and should find ways to communicate this sensitivity on their e-services sites. The government might therefore consider using multiple strategies in order to decrease citizens’ e-privacy concerns. Citizens should then be made aware of these in order to build the required level of trust and confidence in these services.

The study also highlighted the importance of e-privacy awareness in the success of e-government services projects. Increased awareness of risks leads to increased concerns and decreased trust in e-government services. Therefore it is important that there should be comprehensive awareness efforts that counter possible concerns with evidence about the protections that have been put in place. These awareness efforts
should reach all citizens and not only promote the new services but also help citizens to be proactive in adopting e-government services efficiently and safely. This will enhance the chance of success of the implementation.

Protection measures such as modification of the existing laws and legislation to cater for the new e-services, and adopting security technologies (e.g. encryption, smart cards, and other security solutions) are also ways to boost the trustworthiness of e-government services and increase the use of these services. These recommendations are consistent with those of Gartner (2002b). The Gartner recommendations were based on consultancy experience in other countries. It is valuable to have them confirmed with an objective larger scale in-country study. The study reported on in this thesis is the first extensive study that directly reports Oman’s citizens’ perceptions.

Whilst perceived usefulness of e-government services is important, the perceived trustworthiness of e-government services was found to play a more important role in citizens’ intentions to use e-government services. Therefore it is important that governments encourage citizens’ to trust e-government services by boosting their confidence levels before asking them to use the services. The study therefore recommends that governments put strong protection measures in place and ensure that citizens are well informed about them. Gradually deploying effective awareness efforts would deal with raising e-privacy awareness and enhancing e-privacy protection measures (both technical and non technical) would increase citizens’ perceptions of the trustworthiness of e-government services. These recommendations are consistent with opinions provided by the interview participants (see Section 6.8 and Section 7.5).
The study’s participants also made some other general recommendations to the Omani government which they thought would increase the chance of success of the e-government project. These recommendations are not the main focus of this thesis but may make a valuable contribution to the success of e-government implementation.

These recommendations are:

- Provide more e-payment gateways and increase their security as they form the core of e-government services;
- Narrow the digital divide through increasing ICT education and providing better ICT infrastructure spread across the country;
- Expand ICT training to enhance the ICT skills of adolescents so that they will have the capabilities required to adapt well to e-government;
- Increase cross government unit collaboration and cooperation so that there is better service integration and more reliability in service provision.

8.6. The research conclusion

The recent huge advancement in the Internet world has enlarged the risks to e-privacy. E-privacy risk concerns are citizens’ concerns regarding potential loss of control over personal information, such as when information about the citizen is used without permission while using e-government services. Oman is at the initial stage of establishing a single e-government services portal that aims to deliver e-government services in more reliable and efficient manner. Access to the portal is not limited to Internet access but also covers various access channels such as mobile phones and small screen hand held devices. The portal has been designed to be highly secure to enable a single strong authentication process. E-privacy concerns in Oman are also at an early stage but growing along with the expansion of the e-services used by citizens and
residents of Oman. ITA is responsible for handling all IT aspects of the implementation.

The primary objective of this research was to examine the impact of the online privacy concerns on citizens’ acceptance of e-government services. The study developed and tested a model to meet the research objectives and answer its research questions. The model was tested using quantitative and qualitative data analysis. The model represented the influences of e-privacy risk concerns, perceived protection from e-privacy risks, trustworthiness of e-government services, and perceived usefulness of e-government services on citizens’ intentions to use e-government services. It was found that most of the results from the quantitative analysis were consistent with those from the qualitative analysis. Seven of the 11 proposed hypotheses were supported by this study.

The study answered the research question as initially planned. E-privacy risks concerns were found to have an influence on the intention to use e-government service through perceived trustworthiness of e-government services. However, this influence was not a strong one and other factors such as e-privacy protection and social norms were found to play a more important role in influencing the intention to use e-government services.

The study has made a major contribution to scholarly knowledge by providing a more comprehensive model of e-government use and adoption. In particular it has clarified the nature of e-privacy awareness and explained its role in influencing citizens’ intentions to use e-government services. Previous research in the e-commerce domain has explored the role of risk awareness (including e-privacy awareness) in general, but
there has been little research that has specifically examined the role of e-privacy awareness.

There were not many limitations to the research except that e-government services in Oman were fairly new to the citizens and hence it would be a good idea to run the study again in the future. Also the use of only government employees for the sampling frame should be addressed in future research.

Overall, the study found that e-privacy risk concerns and perceptions of the protection available to deter risks influence citizens’ intentions to use e-government services via their influence on the perceived trustworthiness of these services. Other factors such as perceived usefulness, social norms, e-privacy awareness directly or indirectly impact the intention to use e-government services. It was interesting to note that the influence of perceived usefulness of e-government services was only about half as strong as that of perceived trustworthiness. Whilst the intentions of the citizens of Oman to use e-government services are influenced by how useful they believe these services are, the trustworthiness of the services appears to be an even more important issue to them. Therefore the study recommends that governments pay greater attention to the role of e-privacy concerns and put in place security and e-privacy controls. Citizens should then be made aware of these in order to build the required level of trust and confidence in these services. Although the research recommendations were made to the Omani government, they could be applicable to other governments.
Appendix A: English version of the questionnaire
Examining the impact of E-privacy risk concerns on citizens' intentions to use E-government services: An Oman perspective

Survey by Questionnaire

Form Seq. No. (  )

Oman Survey - 2007

By: Dhiyab Al Abri
Australia Mobile: +61 414168413
Email: dalabri@hotmail.com
Dear Participant,

I am a PhD student at Murdoch University, under the supervision of Dr Tanya McGill and Dr Michael Dixon. Oman has been implementing a plan to establish the ‘Oman e-Society vision’. This includes the E-government project, which is intended to facilitate Omani society by supporting most commercial, political, and social online transactions and services. **This research project concerns the possible effect of E-privacy issues on citizens’ usage of E-government services in Oman.**

You are kindly requested to participate in this questionnaire which will take approximately 20 minutes to complete. Completion of the questionnaire is entirely voluntary and you can decide not to participate at any time simply by not completing and submitting the questionnaire. This survey has received Murdoch University's Human Research Ethics Committee approval. All information given during the survey is confidential, and no names or other information that might identify you will be obtained.

This survey consists of two data collection instruments that are this questionnaire and some follow up semi-structured interviews of selected and interested individuals, so if you would like to further participate in the planned interviews please contact me using the contact information below and an appropriate arrangement will be set based on your convenience.

The results of this project will advance the understanding of E-privacy awareness in Oman and may therefore lead to enhance E-government adoption and use. If you wish to further comment on any question or you have any concerns about this survey, please feel free to contact me, Dhiyab Al Abri (Oman Mobile:+968 9947 5030, Australia Mobile:+61414168413, dalabri@hotmail.com, dhiyabalabri@yahoo.com), or my supervisors (Tanya McGill, T.Mcgill@murdoch.edu.au, +61893602798; Michael Dixon, M.Dixon@murdoch.edu.au, +61893606086). Or alternatively if you wish to talk to an independent person about your concerns, you can contact Murdoch University's Human Research Ethics Committee (+61 9360 6677, ethics@murdoch.edu.au).
Definitions of terms used in this study:

<table>
<thead>
<tr>
<th>Term:</th>
<th>Lay Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Site</td>
<td>It is a related collection of World Wide Web (WWW) files that includes a beginning file called a home page. For example the Royal Oman Police <a href="http://www.rop.gov.om">www.rop.gov.om</a></td>
</tr>
<tr>
<td>E-government</td>
<td>The use of Information Technology and Communication infrastructure ability by government units to transform relations with citizens and businesses electronically.</td>
</tr>
<tr>
<td>E-government service</td>
<td>Any service that is made available by the government via the Internet to save time and make citizens’ lives more convenient, for example the Higher Education Admissions Online <a href="http://www.heac.gov.om">www.heac.gov.om</a>.</td>
</tr>
<tr>
<td>E-privacy</td>
<td>The expectations of individuals that their online personal data should generally not be available to others without their prior consent and approval.</td>
</tr>
</tbody>
</table>

Background about E-government services in Oman:

Oman is in the initial stages of implementing the E-government service project as a portion of the E-Oman national project. This project is executed through the Information Technology Authority of Oman (ITA) as appointed by the royal decree number 52/2006.

Although most Omani E-government sites are relatively new, most of them have made great efforts to provide citizens not only with online information but with all possible E-services. A comprehensive list of E-government sites available to Omani citizens can be located at this link: http://www.omannews.com/. Royal Oman Police www.rop.gov.om is among those sites that facilitate citizens with online services and comprehensive information, as it allows citizens to query their possible traffic fines and has most of the Omani laws online readily for download and/or browsing.

According to ITA http://www.ita.gov.om/english/government.html, Oman is doing what it takes to accelerate the steps towards having most of the government services online through the national UBAR by 2010. In this sense ITA is working on many E-government projects side by side with individual government units. Some of these projects, such as the National Registry and Higher Education Registry Centre site www.heac.gov.om, are already in place for citizens and others are underway, such as the E-payment gateway, E-tendering, E-government services for companies and the National Educational Portal. In all, Oman is looking forward to having most of the government services in the unified portal within the coming three years or so.
Part A. Demographic and Background Information

This portion of the questionnaire collects some basic demographic and background information about you. Please select only one answer for each of the following questions.

1. How old are you?
   - 1. 18-29
   - 2. 30-49
   - 3. 50+

2. What gender are you?
   - 1. Female
   - 2. Male

3. What level of education do you have?
   - 1. High School or less
   - 2. Some College
   - 3. Graduate
   - 4. Post graduate

4. Which statement best describes your level of experience of using the World Wide Web?
   - 1. None
   - 2. Beginner
   - 3. Intermediate
   - 4. Advanced

5. Which statement best describes your level of experience of using E-government services?
   - 1. None
   - 2. Beginner
   - 3. Intermediate
   - 4. Advanced

6. Have you taken a formal Internet usage skills course (e.g. at school, at work, vocational training)?
   - 1. Yes
   - 2. No

Part B. E-government Usefulness of E-government Services

B1. This portion of the questionnaire relates to how useful you think Omani E-government services would be in enhancing your knowledge/transaction performance. Please select only one answer for each of the following questions.

7. E-government sites would provide valuable services for me.
   - 1. Strongly Disagree
   - 2. Disagree
   - 3. Neutral
   - 4. Agree
   - 5. Strongly Agree

8. The content of the E-government sites would be useful to me.
   - 1. Strongly Disagree
   - 2. Disagree
   - 3. Neutral
   - 4. Agree
   - 5. Strongly Agree

9. E-government services would enhance my effectiveness in searching for government information.
   - 1. Strongly Disagree
   - 2. Disagree
   - 3. Neutral
   - 4. Agree
   - 5. Strongly Agree

1 Strongly Disagree  2 Disagree  3 Neutral  4 Agree  5 Strongly Agree

11. Using E-government services would increase my overall productivity.

1 Strongly Disagree  2 Disagree  3 Neutral  4 Agree  5 Strongly Agree

12. Using E-government services would make it easier to interact with the government.

1 Strongly Disagree  2 Disagree  3 Neutral  4 Agree  5 Strongly Agree

B2. The following questions relate to other peoples’ opinion of your use of Omani E-government services sites. Please select only one answer for each question.

13. My family think I should use the E-government services.

1 Strongly Disagree  2 Disagree  3 Neutral  4 Agree  5 Strongly Agree

14. My colleagues think I should use the E-government services.

1 Strongly Disagree  2 Disagree  3 Neutral  4 Agree  5 Strongly Agree

15. My friends think I should use the E-government services.

1 Strongly Disagree  2 Disagree  3 Neutral  4 Agree  5 Strongly Agree

16. People I know think that using the E-government services is a good idea.

1 Strongly Disagree  2 Disagree  3 Neutral  4 Agree  5 Strongly Agree

Part C Prior E-services Experience

This portion of the questionnaire relates to your level of experience in using Internet sites to conduct online transactions to receive services from public or private organization web sites.

17. I frequently use the Internet to find information about services and products

1 Strongly Disagree  2 Disagree  3 Neutral  4 Agree  5 Strongly Agree

18. I frequently pay for products or services on the Internet using E-services sites

1 Strongly Disagree  2 Disagree  3 Neutral  4 Agree  5 Strongly Agree

19. Many times I have requested further information about certain products or services on the Internet

1 Strongly Disagree  2 Disagree  3 Neutral  4 Agree  5 Strongly Agree

20. I have disclosed my personal information to E-services sites several times

1 Strongly Disagree  2 Disagree  3 Neutral  4 Agree  5 Strongly Agree
21. So far, I have conducted many E-services through the available websites
1 Strongly Disagree  2 Disagree  3 Neutral  4 Agree  5 Strongly Agree

**Part D: E-Privacy Risk Concerns and Perceived E-privacy Protections**

**D1.** This portion of the questionnaire relates to any E-privacy concerns you may have about using Omani E-government service. Please select only one answer for each of the following questions.

22. I'm concerned that E-government sites will collect too much personal information about me.
1 Strongly Disagree  2 Disagree  3 Neutral  4 Agree  5 Strongly Agree

23. It would bother me if E-government sites ask for personal information.
1 Strongly Disagree  2 Disagree  3 Neutral  4 Agree  5 Strongly Agree

24. E-government sites should not use personal information for any purpose unless it has been authorized by the individuals who provided the information.
1 Strongly Disagree  2 Disagree  3 Neutral  4 Agree  5 Strongly Agree

25. If E-government sites ask me for personal information, I would think twice before providing it.
1 Strongly Disagree  2 Disagree  3 Neutral  4 Agree  5 Strongly Agree

26. E-government sites should take more steps to make sure that the personal information in their files is accurate.
1 Strongly Disagree  2 Disagree  3 Neutral  4 Agree  5 Strongly Agree

27. E-government sites should have better procedures to correct errors in personal information.
1 Strongly Disagree  2 Disagree  3 Neutral  4 Agree  5 Strongly Agree

28. E-government sites should never share personal information with other government units unless it has been authorized by the individuals who provided the information.
1 Strongly Disagree  2 Disagree  3 Neutral  4 Agree  5 Strongly Agree

29. E-government sites should take more steps to make sure that unauthorized people cannot access personal information in their computers.
1 Strongly Disagree  2 Disagree  3 Neutral  4 Agree  5 Strongly Agree
D2. This portion of the questionnaire relates to how much you know about possible E-privacy risks of using Omani E-government services. Please select only one answer for each of the following questions.

30. I am aware of E-privacy risks.
   - [ ] Strongly Disagree
   - [ ] Disagree
   - [ ] Neutral
   - [ ] Agree
   - [ ] Strongly Agree

31. I am aware that whenever I give my personal information to any E-government site it could be accessed by many others.
   - [ ] Strongly Disagree
   - [ ] Disagree
   - [ ] Neutral
   - [ ] Agree
   - [ ] Strongly Agree

32. I am aware that my personal information could be transmitted to other government units.
   - [ ] Strongly Disagree
   - [ ] Disagree
   - [ ] Neutral
   - [ ] Agree
   - [ ] Strongly Agree

33. I am aware that my personal information given to E-government sites could be used to track my online behaviour.
   - [ ] Strongly Disagree
   - [ ] Disagree
   - [ ] Neutral
   - [ ] Agree
   - [ ] Strongly Agree

D3. This portion of the questionnaire relates to perceived e-privacy protection of your information. Please select only one answer for each of the following questions.

34. E-government sites will devote time and effort to preventing unauthorized access to my personal information.
   - [ ] Strongly Disagree
   - [ ] Disagree
   - [ ] Neutral
   - [ ] Agree
   - [ ] Strongly Agree

35. I feel that E-government sites will not release personal information about me without my express permission.
   - [ ] Strongly Disagree
   - [ ] Disagree
   - [ ] Neutral
   - [ ] Agree
   - [ ] Strongly Agree

36. I feel that E-government sites would make a reasonable effort to ensure that the information collected about me is accurate.
   - [ ] Strongly Disagree
   - [ ] Disagree
   - [ ] Neutral
   - [ ] Agree
   - [ ] Strongly Agree

37. E-government sites would give me a clear choice before disclosing personal information about me to third parties.
   - [ ] Strongly Disagree
   - [ ] Disagree
   - [ ] Neutral
   - [ ] Agree
   - [ ] Strongly Agree

38. E-government sites would have a mechanism to review and change incorrect personal information.
   - [ ] Strongly Disagree
   - [ ] Disagree
   - [ ] Neutral
   - [ ] Agree
   - [ ] Strongly Agree
Part E: E-government Services Trustworthiness

This portion of the questionnaire relates to your confidence that E-government services sites in Oman will be reliable and fully integrated to protect your E-privacy. Please select only one answer for each of the following questions.

39. In general, the Internet is now a robust and safe environment for E-government services transactions.

1 [ ] Strongly Disagree  2 [ ] Disagree  3 [ ] Neutral  4 [ ] Agree  5 [ ] Strongly Agree

40. The Internet has enough safeguards to make me feel comfortable using it to interact with the government.

1 [ ] Strongly Disagree  2 [ ] Disagree  3 [ ] Neutral  4 [ ] Agree  5 [ ] Strongly Agree

41. I think I trust Omani E-government services sites.

1 [ ] Strongly Disagree  2 [ ] Disagree  3 [ ] Neutral  4 [ ] Agree  5 [ ] Strongly Agree

42. I think Omani E-government sites will be trustworthy.

1 [ ] Strongly Disagree  2 [ ] Disagree  3 [ ] Neutral  4 [ ] Agree  5 [ ] Strongly Agree

43. Omani E-government sites will keep citizens’ best interests in mind.

1 [ ] Strongly Disagree  2 [ ] Disagree  3 [ ] Neutral  4 [ ] Agree  5 [ ] Strongly Agree

44. E-privacy security policies and precautions of Omani E-government sites will make me feel that the services are trustworthy.

1 [ ] Strongly Disagree  2 [ ] Disagree  3 [ ] Neutral  4 [ ] Agree  5 [ ] Strongly Agree

Part F: Intention to Use E-government Services

This portion of the questionnaire relates to your intentions to use Omani E-government sites. Please select only one answer for each of the following questions.

45. I would use the E-government services to gather governmental information.

1 [ ] Strongly Disagree  2 [ ] Disagree  3 [ ] Neutral  4 [ ] Agree  5 [ ] Strongly Agree

46. I would use E-government services provided over the web.

1 [ ] Strongly Disagree  2 [ ] Disagree  3 [ ] Neutral  4 [ ] Agree  5 [ ] Strongly Agree

47. Interacting with the government over the web is something that I would do.

1 [ ] Strongly Disagree  2 [ ] Disagree  3 [ ] Neutral  4 [ ] Agree  5 [ ] Strongly Agree
48. I would be willing to provide personal information to E-government sites.
   1  Strongly Disagree  2  Disagree  3  Neutral  4  Agree  5  Strongly Agree

49. I would be willing to recommend others to use and disclose their personal information to E-government sites to interact with government through the e-government sites.
   1  Strongly Disagree  2  Disagree  3  Neutral  4  Agree  5  Strongly Agree

**Part G: Actual E-government Use**

*This portion of the questionnaire relates to your actual usage of Omani E-government services sites. Please select only one answer for each of the following questions.*

50. I frequently interact with the government through E-government services sites.
   1  Strongly Disagree  2  Disagree  3  Neutral  4  Agree  5  Strongly Agree

51. I have disclosed my personal information to E-government sites several times.
   1  Never  2  Seldom  3  About half the time  4  Usually  5  Always

52. I frequently pay for government services through E-government sites.
   1  Never  2  Seldom  3  About half the time  4  Usually  5  Always

53. The best statement to describe my actual use of E-government services is
   1  No use of E-government services sites at all.
   2  To get government information only.
   3  To get information and to conduct essential transactions only whenever there is no other way to get the service.
   4  To get information and to conduct transactions regularly.

54. On average each month, how many hours do you spend using E-government services sites? (----- Hr(s))
   1  0 - 12  2  12 - 17  3  18-23  4  24-30  5  more than 30

55. How long have you been using E-government services in Oman? (---- Months)
   1  0 - 5  2  6 - 10  3  11 - 15  4  16 - 20  5  more than 20

56. Over the past 12 months, approximately how much have you paid via E-government sites for government services? (------ R.O.)
   1  0  2  1-100  3  101-500  4  500-1000  5  more than 1000
If you have further comments about the subject of the questionnaire, please indicate them below:
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
This survey consists of two data collection instruments that are this questionnaire and some follow up interviews of selected individuals’.

Would you like to participate in the planned interviews?

☐ 1   No
☐ 2   Yes (please contact the researcher on the given contact information shown in the beginning of this questionnaire)

Your contribution to this survey is very greatly appreciated.

I would like to have a summary report compiled from this survey

☐ 1   No
☐ 2   Yes (please contact the researcher on the given contact information shown in the beginning of this questionnaire)

(Thank you for your time.)
Appendix B: The Arabic version of the questionnaire
Examining the impact of E-privacy risk concerns on citizens' intentions to use E-government services: An Omani perspective

الباحث: ذياب بن سالم العري

رقم الهاتف: (استراليا 61414168413 + 96899475030 + عمان)
dalabri@hotmail.com Email:
عزيزي المشارك،

هذه الاستبانة جزء من مطالبات نيل شهادة الدكتوراه في مجال تقييم المعلومات من جامعة مردوخ و بإشراف كل من الدكتوركة تانيا ميجل و الدكتور مايكل ديكسون. تأتي هذه الدراسة مزمنة مع تطبيق سلطة عمان لرؤية المجتمع الرقمي بما فيه من مشاريع للحكومة الإلكترونية هدف الحكومة الإلكترونية في عمان توفير مظلات الخدمات الإلكترونية باستخدام الإنترنت لكافة شرائح المجتمع السياسية، الاجتماعية، والتجارية وكذا ما يكلف سرعة الاتصال ورفع كفاءة الأداء.

تذكر هذه الدراسة على جوانب تأثير فائق المواطين من محاكتن احتراق تخصصية البيانات الشخصية أثناء استخدام خدمات الحكومة الإلكترونية وما يتبع ذلك من تداعيات في إيجاح هذه المشاريع الوطنية. لهذا ينصحنا الفلسفة في تقديم ما هو جديد في مجال فهم متطابقات التخصصية الفردية اللازمة لتعزيز مواطن ليتني خدمات الحكومة الإلكترونية في سلطنة عمان.

برجاء التكرم بالمشاركة في هذه الدراسة من خلال تعنيضة الاستنبال المرفق والتي نأمل أنها تشمل لك الإجازة على ما أكثر من 20 دقيقة علميا بأن المشاركة في هذه الاستبانة هي عمل اختياري وحيد بينما ندعوكم لا كمال الإجازة عليها إلا أنه ننصح بالتوافق عن إكمالها لما بقي من وقت الحاجة ملحة لذلك نتذرر الإشارة هنا بأن هذه الاستبانة قد حصلت على موافقة لجنة أخلاقيات البحث العلمي بجامعة مردوخ و لن يتم قبول أي بيانات شخصية تدل على المشاركة في أي جزء من أجزاء الاستبانة كما أكمل ذلك أن مشاركات هذه الدراسة بما فيها من نتائج سوف تتألف بسرية كاملة و لن يحق لفودي الباحث و مستفيدي الاطلاع عليها.

نود أيضاً أن نتمكن بأن مجموعة من المقابلات الشخصية المتبقية من الاستبانة بعد عرض نتائجها و ذلك هدف تنويع مصادر البيانات و تعدد طرق جمعها مما إذا رغبت في المشاركة في المقابلات الشخصية فإنه يمكن الاتصال بالباحث من خلال بيانات الاتصال أدناه و نستند الاتصال بالبحث للعديد المطلوب للمقابلة في حالة وجود أي استفسار أو إسهام أو ملاحظة على هذه الاستبانة فإنه يمكن الاتصال بالباحث على أحد العنايين التالي ( عمان 3099475030 أو استراليا 61414184613) dhiyabalabri@yahoo.com (dalabri@hotmail.com
( M.Dixon@murdoch.edu.au T.Mcgill@murdoch.edu.au ethics@murdoch.edu.au

الاتصال بلجنة الأخلاقيات البحث العلمي في جامعة مردوخ على (777)618936066677+189
### المصطلح

<table>
<thead>
<tr>
<th>المصطلح</th>
<th>الوصف</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Web Site) الموقع الإلكتروني</td>
<td>مجموعة من الصفحات الإلكترونية على الشبكة العالمية &quot;الإنترنت&quot; التي تمثل الموقع الإلكتروني لمؤسسة متمثلة بشرطة عمان السلطانية <a href="http://www.rop.gov.om">www.rop.gov.om</a></td>
</tr>
<tr>
<td>الحكومة الإلكترونية (E-government)</td>
<td>استخدام الوحدات الحكومية لإمكانات وسائل الاتصال وتقيمة المعلومات لتوفير خدماتها المختلفة للمواطن ومؤسسات التجارة الإلكترونية عن طريق الإنترنت</td>
</tr>
<tr>
<td>(E-service) الخدمة الإلكترونية</td>
<td>الخدمة المقدمة من قبل المؤسسات سواء الحكومية أو غير الحكومية المختلفة الإلكترونية عبر مواقع الإنترنت مثل سداد الفواتير وتجديد الرخص وشراء البضائع و... و الخ</td>
</tr>
<tr>
<td>خدمات الحكومة الإلكترونية (E-government services)</td>
<td>أي خدمات متاحة إلكترونياً من قبل الحكومة محددة تسريع الإجراءات و الوثائق والخدمات مثل سجل القبول الموحد <a href="http://www.heac.gov.om">www.heac.gov.om</a></td>
</tr>
<tr>
<td>الخصوصية الإلكترونية (E-Privacy)</td>
<td>مطالبة مستخدم الإنترنت لضمان عدم اطلاع أو استخدام البيانات الخاصة به بدون سابق علمه موافقة.</td>
</tr>
</tbody>
</table>
مقديمة تعريفية عن خدمات الحكومة الإلكترونية في سلطنة عمان

يتم حاليا تنفيذ و تشغيل مشروع الحكومة الإلكترونية في السلطنة ضمن منظومة مشروع جميع عمان الرقمي و الذي تشرف عليه الهيئة العامة لتقنية المعلومات التي انشئت بموجب المرسوم السلطاني رقم(52/2006).

رغم أن معظم مواقع الوحدات الحكومية الإلكترونية تعد حديثة نوعا ما إلا أنها قطعت شوطا كبيرا في توفير ليس فقط الكثير من المعلومات و الاعيان الإلكترونية بل و الكثير من الخدمات الإلكترونية وتقتربا معظم الوحدات الحكومية توفير المعلومات الخاصة بخدماتها الإلكترونية وفق الوصلة التالية:

http://www.omannews.com/?lang=fa

و يعد مواقع شرطة عمان السلطانية من بين المواقع الشائعة الاستخدام في مجال التواصل مع الجهات الحكومية من خلال توفير خدمة معرفة مخالفات المرور و توفر معظم قوائمها المستخدمة في موقعها الرسمي و هناك أيضا العديد من المواقع الحكومية التي توفر أو تسعي توفير خدمات الالكترونية مثل الشبكة الحكومية الموحدة و بوابة أوبار خدمات الحكومة الإلكترونية و السجل المدني و التنافس الالكتروني و بوابة المدفوعات الالكترونية و الخدمات الحكومية التجارية و مركز الفوائد الموحد و البوابة التعليمية وفق ما ورد في موقع هيئة تقنية المعلومات على الوصلة التالية:


الوصلة التالية:
الجزء الأول: البيانات démographique et الأولى

هذا الجزء من الاستمارة يحتوي على بيانات démographique et الأولى عن المشاركة، من فضلك اختر اجابة واحدة فقط.

1. إلى أي الفئات العمرية التالية تنتمي؟
   □ 18-29 □ 30-49 □ 50 +
   □ 1 □ 2 □ 3 □ 4 □ 5

2. ما جنسك؟
   □ ذكر □ أنثى

3. ما مستوى التعليم?
   □ الشهادة العامة وما فوق □ دون الجامعي □ مستوى الجامعة □ المستوى فوق الجامعي

4. ما مستوى خبرتك في مجال استخدام شبكة الإنترنت?
   □ لا يوجد □ مبتدئ □ متوسط □ مقدم

5. ما مستوى خبرتك في مجال استخدام مواقع الخدمات الإلكترونية؟
   □ لا يوجد □ مبتدئ □ متوسط □ مقدم

6. هل سبق أن حصلت على تدريب متخصص في مجال تقنية المعلومات في (العمل، المدرسة، معهد مدني، .. الخ)
   □ نعم □ لا

الجزء الثاني: الفوائد المتوقعة للحكومة الإلكترونية

لبتلقى هذا الجزء من الاستمارة بمعرفة وجهة نظرك في مدى فائدة استخدام خدمات الحكومة الإلكترونية في رفع المستوى المعرفي ورفع كفاءة الخدمات الحكومية، من فضلك اختر اجابة واحدة فقط لكل من الآتي.

7. ستتوفر لي الحكومة الإلكترونية خدمات ثمينة
   □ لا أوافق بشدة □ لا أوافق □ محايد □ أوافق □ أوافق بشدة

8. سيكون محتوى مواقع الحكومة الإلكترونية مفيد لي
   □ لا أوافق بشدة □ لا أوافق □ محايد □ أوافق □ أوافق بشدة

9. سترفع خدمات الحكومة الإلكترونية من معدل كفاءتي عند البحث عن المعلومات الحكومية
   □ لا أوافق بشدة □ لا أوافق □ محايد □ أوافق □ أوافق بشدة

10. سيزيد معدل كفاءتي في تحليل معاملاتي الحكومية باستخدام مواقع خدمات الحكومة الإلكترونية.
11. استخدام مواقع الحكومة الإلكترونية سيرفع من معدل كفاءة الإنجاز لدى بشكل عام

12. سرعان مع بعض المؤسسات الحكومية

13. تعتقد عائلتي بأنه ينبغي علي أن استخدم الحكومة الإلكترونية

14. يعتقد ملاحي في العمل بأنه ينبغي علي أن استخدم خدمات الحكومة الإلكترونية

15. يعتقد أصدقائي بأنه ينبغي علي أن استخدم الحكومة الإلكترونية

16. يعتقد الناس المقربين مني إن استخدام خدمات الحكومة الإلكترونية فكرة جيدة

17. تعودت على استخدام الإنترنت للحصول على معلومات الالكترونية عن الخدمات والبضائع

18. تذكرني نستعمل وسائل الدفع الالكترونية بواسطة الإنترنت للحصول على بضائع وخدمات الالكترونية

الجزء الثالث: الخبرة في استخدام الخدمات الالكترونية

يعتبر هذا الجزء من الاستمارة بمجرد مستوى معياري يتطلب في مجال استخدام مواقع الخدمات الالكترونية لإنجاز معاملات الالكترونية سواء كان ذلك مع المؤسسات الخاصة أو العامة، من فضلك اختر إجابة واحدة فقط من الآتي.

193
19. لعدة مرات قمت بطلب مزيد من المعلومات عن خدمات و بضائع متاحة عن طريق خدمات الإنترنت
لا أوافق بشدة □ لا أوافق □ محباً □ أوافق □ أوافق بشدة □

20. قمت بالإفصاح عن بيانات شخصية خاصة لمواقع الخدمات الإلكترونية لعدة مرات
لا أوافق بشدة □ لا أوافق □ محباً □ أوافق □ أوافق بشدة □

21. حتى الآن، قمت بإنجاز العديد من المهام باستخدام مواقع الخدمات الإلكترونية المتاحة
لا أوافق بشدة □ لا أوافق □ محباً □ أوافق □ أوافق بشدة □

الجزء الرابع: المخاوف المتعلقة بالخصوصية الإلكترونية و متطلبات الحماية

آ. يتعلق هذا الجزء من الاستطلاع ببعض من مخاطر اختراق خصوصياتك الشخصية في الإنترنت عند استخدام مواقع الخدمات الإلكترونية لإرسال معلوماتك الحكومية (العامة)، من فضلك اختر إجابة واحدة فقط لكل من الآتي. √

22. أشعر بالقلق حين تقوم مواقع الحكومة الإلكترونية بتجميع بيانات شخصية كثيرة علي
لا أوافق بشدة □ لا أوافق □ محباً □ أوافق □ أوافق بشدة □

23. لا أشعر بالإرتياح عند قيام مواقع الحكومة الإلكترونية بمطالبي ادخال بياناتي الشخصية الخاصة
لا أوافق بشدة □ لا أوافق □ محباً □ أوافق □ أوافق بشدة □

24. ينبغي على مواقع الحكومة الإلكترونية استخدام بياناتي الشخصية الخاصة بي في غير الغرض المحدد بدون سابق موافقتي و معرفتي
لا أوافق بشدة □ لا أوافق □ محباً □ أوافق □ أوافق بشدة □

25. في حال طلبية مواقع الحكومة الإلكترونية ببياناتي الخاصة سافكر ملباً وأكثر من مرة قبل تزويدها بالبيانات المطلوبة
لا أوافق بشدة □ لا أوافق □ محباً □ أوافق □ أوافق بشدة □

26. ينبغي على مواقع الحكومة الإلكترونية اتخاذ مزيد من التدابير لضمان صحة و تكامل البيانات لديها
لا أوافق بشدة □ لا أوافق □ محباً □ أوافق □ أوافق بشدة □
27. ينبغي على مواقع الحكومة الإلكترونية اتخاذ مزيدًا من التدابير الأمنية لتصحيح الأخطاء المحتملة في ملفات البيانات الإلكترونية الموجودة لديها.

لا أوافق بشدة ☐ لا أوافق ☐ محابلد ☐ أوافق ☐ أوافق بشدة ☐

28. ينبغي على مواقع الحكومة الإلكترونية مشاركة الوحدات الحكومية الأخرى في البيانات الخاصة بالمواطنين والمجمعة بواسطة هذه المواقع إلا بحلف صاحب الشأن والأخ موافقته المسبقة.

لا أوافق بشدة ☐ لا أوافق ☐ محابلد ☐ أوافق ☐ أوافق بشدة ☐

29. يتوجب على مواقع الحكومة الإلكترونية اتخاذ مزيدًا من التدابير الأمنية لضمان عدم استخدام بيانات المواطنين في ملفاتها الإلكترونية من قبل الأفراد غير المحولين بذلك.

لا أوافق بشدة ☐ لا أوافق ☐ محابلد ☐ أوافق ☐ أوافق بشدة ☐

30. إذا لم يتم مخاطر اختراق الخصوصية الشخصية في شبكة الإنترنت.

لا أوافق بشدة ☐ لا أوافق ☐ محابلد ☐ أوافق ☐ أوافق بشدة ☐

31. إذا على المالم ودراسة تامة بأن بياناتي المطاطة إلى مواقع الحكومة الإلكترونية قد تكون معرضة للاستخدام من قبل آخرين من غير المصنوع لهم، ولقي معرفين لدي.

لا أوافق بشدة ☐ لا أوافق ☐ محابلد ☐ أوافق ☐ أوافق بشدة ☐

32. إذا على وعي كام بأن بياناتي المطاطة إلى مواقع الحكومة الإلكترونية قد تحتاج للاستخدام من قبل وحدات حكومية وإدارية أخرى.

لا أوافق بشدة ☐ لا أوافق ☐ محابلد ☐ أوافق ☐ أوافق بشدة ☐

33. إذا على وعي كام بأن بياناتي المطاطة إلى مواقع الحكومة الإلكترونية قد تستخدم في تطبيع سلوكي الشخصي في الإنترنت.

لا أوافق بشدة ☐ لا أوافق ☐ محابلد ☐ أوافق ☐ أوافق بشدة ☐

34. يتعلق هذا الجزء من الاستنادية بحماية الخصوصية الشخصية من مخاطر الاختراق عند استخدام مواقع الحكومة الإلكترونية، من خلال اختراق إجابة وحادة نقطة لكل من الأتي.

لا أوافق بشدة ☐ لا أوافق ☐ محابلد ☐ أوافق ☐ أوافق بشدة ☐

35. في اعتراف بأن مواقع الحكومة الإلكترونية لن تقوم بالتصريح عن بياناتي الشخصية إلا بموجب موافقة المعتادة.
في اعتقادي بأن مواقع الحكومة الإلكترونية سوف تقوم بكل ما في وسعها لتصحيح بيانات
الشخصية المجمعة لديها قبل الاعتماد عليها في أي إجراء

37. ستقوم مواقع الحكومة الإلكترونية بإعطاء الحرية الكاملة والمطلقة للاختيار قبل
افصاحها عن بياناتي الشخصية لأي طرف ثالث

38. سيكون لدى مواقع الحكومة الإلكترونية أليات محددة لمراجعة وتدقيق بياناتي الشخصية
المسجلة لديها لضمان صحتها وتكاملها

39. تعد اليوم بيئة الإنترنت بينة أمنة ل كافة استخدامات الحكومة الإلكترونية بشكل عام

40. تتمتع بيئة شبكة الإنترنت بوسائل حماية إلكترونية وقانونية كافية مما يعود إلى
الاطمئنان لاستخدام خدمات الحكومة الإلكترونية

41. أعتقد بأن أثق في مواقع الحكومة الإلكترونية في عمان

42. أعتقد بأن مواقع الحكومة الإلكترونية جيدة بالثقة في مجال الخصوصية الفردية بشكل عام

43. ستوتي مواقع الحكومة الإلكترونية في عمان مصلحة المواطنين جل اهتمامها

44. تعد مواقع الحكومة الإلكترونية موثوقة وبالتالي ينبغي الاعتماد عليها

الجزء الخامس: الوثائق في خدمات الحكومة الإلكترونية

 يتعلق هذا الجزء من الاستياء بمعرفة مدى جدارة مواقع الحكومة الإلكترونية بتفقد إنجاز معلماً
 الحكومية الإلكترونية، من فضلك اختر إجابة واحدة فقط لكل من الأسئلة.

1. لا أوافق بشدة 2. لا أوافق 3. محدود 4. أوافق 5. أوافق بشدة

2. لا أوافق بشدة 2. لا أوافق 3. محدود 4. أوافق 5. أوافق بشدة

3. لا أوافق بشدة 2. لا أوافق 3. محدود 4. أوافق 5. أوافق بشدة

4. لا أوافق بشدة 2. لا أوافق 3. محدود 4. أوافق 5. أوافق بشدة

5. لا أوافق بشدة 2. لا أوافق 3. محدود 4. أوافق 5. أوافق بشدة

6. لا أوافق بشدة 2. لا أوافق 3. محدود 4. أوافق 5. أوافق بشدة
الجزء السادس: نية المواطن في استخدام الحكومة الإلكترونية

يتطلب هذا الجزء من الاستمارة بموافقة أي تطبيق مستقبلية في استخدام مواقع الحكومة الإلكترونية لاتجاز معاملات الحكومة الإلكترونية، من فضلك إختر إجابة واحدة فقط لكل من الآتي.

| لا أوافق بشدة | 2 | لا أوافق | 3 | محايد | 4 | أوافق | 5 |

45. سأستخدم مواقع الحكومة الإلكترونية للحصول على أي معلومات حكومية

46. سأستخدم الخدمات الإلكترونية المتوفرة في مواقع الحكومة الإلكترونية

47. سوف لن أتردد في التعامل مع الحكومة من خلال مواقع الحكومة الإلكترونية

48. سوف لن أتردد في استخدام و تزويد مواقع الحكومة الإلكترونية ببياناتي الشخصية إذا رغبت في أي خدمات حكومية إضافية مستقبلاً

49. سوف أقترح الآخرين عدم التardo في استخدام و تزويد مواقع الحكومة الإلكترونية بالبيانات الشخصية عند رغبتي في التعامل مع الحكومة

الجزء السابع: الاستخدام الفعلي (الحالي) للحكومة الإلكترونية

يتعلق هذا الجزء من الاستمارة بلمحة مدى استخدامات الحالية لموارد الحكومة الإلكترونية لإجراي معاملات الحكومة الإلكترونية، من فضلك إختر إجابة واحدة فقط لكل من الآتي.

| لا أوافق بشدة | 2 | لا أوافق | 3 | محايد | 4 | أوافق | 5 |

50. أنا معتاد على التفاعل مع مواقع الحكومة الإلكترونية للحصول على الخدمات الحكومية

51. سبق لي أن زودت مواقع الحكومة الإلكترونية في عمان ببياناتي الشخصية

■ لا  | 2 | لا  | 3 | محايد | 4 | أوافق | 5 | غالبًا  | دائماً
52. أقوم بدفع رسوم الخدمات الحكومية من خلال مواقع الحكومة الإلكترونية في عمان بشكل مستمر.
53. أفضل عبارة لوصف استخدامي لخدمات مواقع الحكومة الإلكترونية هي
54. أقوم باستخدام خدمات المتوفرة لمواقع الحكومة الإلكترونية فقط.
55. متوسط استخدامي لخدمات مواقع الحكومة الإلكترونية في الشهر؟ (------- ساعة)
56. قيمة الدفع الإلكتروني للخدمات المتوفرة لمواقع الحكومة الإلكترونية خلال الاربعة عشر شهرا الماضية تقريبا؟ (-------- ريال عماني)

* هل ترغب في المشاركة في مقابلات الشخصية التي ستمتبع هذه الاستبانة كجزء من الدراسة الكلية؟

لا 1
نعم 2

* هل يوجد في رسوم الحصول على تقرير بنتائج هذه الاستبانة؟

لا 1
نعم 2
نتمنى لك إسهامك الكبير في إنجاز هذه الدراسة من خلال الإجابة على الاستبانة.
يرجى إعادة الاستبانة إلى دائرة شئون الموظفين أو الموظف المختص.

(شكراً جزيلاً على وقتك الثمين)
Appendix C: The interview guide
Project title: Examining the impact of E-privacy risk concerns on citizens' intentions to use E-government services: An Oman perspective

I am a PhD student at Murdoch University, under the supervision of Dr Tanya McGill and Dr Michael Dixon. Oman has been implementing a plan to establish the ‘Oman e-Society vision’. This includes the an E-government project, which is intended to facilitate Omani society by supporting most commercial, political, and social online transactions and services. This research project concerns the possible effect of E-privacy issues on citizens’ usage of E-government services in Oman.

You are kindly requested to participate in an interview. The interview will take approximately 20 minutes to complete. It is a semi-structured interview where you have the chance to read the questions and write your answers prior to the interview session if you wish. The interview session will be scheduled according to your convenience. Your participation in this interview is entirely voluntary and you can decide not to participate at any time.

This research has received Murdoch University’s Human Research Ethics Committee approval. All information given during the interview is confidential and no names or other information that might identify you will be used in any publication arising from the research.

If you have any questions, comments or concerns about this interview or the research in general, please feel free to contact the researcher Dhiyab Al Abri (+968 9947 5030, +61414168413, dalabri@hotmail.com, dhiyabalabri@yahoo.com). I will be happy to discuss with you any concerns you may have on how this study has been conducted, or you may contact my supervisors (Tanya McGill, T.Mcgill@murdoch.edu.au, +61893602798; Michael Dixon, M.Dixon@murdoch.edu.au, +61893606086). Alternatively if you wish to talk to an independent person about your concerns you can contact Murdoch University's Human Research Ethics Committee on (+6189360 6677, ethics@murdoch.edu.au).

If you are willing to participate in this study, could you please complete the details below?

Thank you.
Dhiyab Al Abri
I (the participant) have read the information above. Any questions I have asked have been answered to my satisfaction. I agree to take part in this interview and for the researcher to voice record my answers, however, I know that I may change my mind and stop at any time.

I understand that all information provided is treated as confidential and will not be released by the investigator unless required to do so by law.

I agree that research data gathered for this study may be published provided my name or other information which might identify me is not used. I also agree that this interview can be tape recorded.

Participant:

Date:

Investigator:

Date:

Investigator's Name:
Interview Guide

Part A: Demographic and background Information
1. How old are you?
2. What is your gender?
3. What education level do you have?
4. Do you use the Internet? How long have you been using it?
5. How would you describe your (Computer, Internet, and E-service) experience?

Part B: E-government in Oman
1. To what extent do you think that E-government is essential to Oman?
2. How would you describe E-government awareness efforts in Oman (adequacy/ comprehensiveness)?
3. In your opinion do you think Omani E-government services project will be successful?
4. To what extent does somebody you know ex. (spouse boss, friend, family member, and colleague) might influence your decision to use E-government services or not?
5. Would you name some E-government services that you have used or that you just know about?

Part C: E-privacy concerns and protection measures
1. How much do you know about E-privacy concerns?
2. Do you have any concerns about your privacy while you are using the Internet and what is your biggest concern?
3. In your opinion, do you think E-privacy will have any impact on the success of E-government service adoption by citizens in Oman?
4. Would you please explain how and to what extent E-privacy might influence your pattern of using E-government services?
5. Can you describe what aspect of E-privacy concerns is having the most impact on citizens’ use of E-government services? Is it different when talking about E-commerce?
6. Do you think that citizens are aware of E-privacy concerns and protection measures, and do you think that this awareness level might make a difference in using E-government services?

7. How would you describe Oman’s E-privacy readiness, in general, and within the E-government project in particular?

8. Do you take any action(s) to protect your E-privacy?

**Part D: Trustworthiness on E-government services**

1. Do you think E-government services in Oman are trustworthy?

2. In relation to E-privacy concerns of E-government services, what is your future intention with respect to use of E-government services?

(Thank you for your time)
Appendix D: Themes selection process
### Themes selection process

<table>
<thead>
<tr>
<th>Research Construct and themes</th>
<th>Participants’ Replays</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>E-privacy Awareness</strong>, know, knowledge, acknowledge</td>
<td><strong>Awareness</strong> efforts in Oman are very low and not sufficient. ITA is doing an appreciated effort. The <strong>awareness</strong> efforts are not enough yet they are in the right direction. I do not think all people need to know much about e-privacy risks and security measures as it is too early now. ITA started since long time. <strong>Awareness</strong> isn’t covering everywhere neither comprehensive. The <strong>awareness</strong> doesn’t cover the <strong>security</strong> aspects. No it is not adequate and not comprehensive. ITA should apply more <strong>awareness</strong> efforts and government information systems should be fully protected. The government is not doing enough efforts to make the citizens aware of online risks. Local classical media channels are not very effective nowadays, therefore, <strong>awareness</strong> should be through the service portal itself. I don’t hear that there is an effective <strong>awareness</strong> effort. To find an excuse for the government, I try to convene my self that the project is not executed yet.</td>
</tr>
<tr>
<td><strong>Experience</strong>, skills</td>
<td>Not at all.</td>
</tr>
<tr>
<td><strong>E-privacy risks concerns</strong></td>
<td>I am with an excellent IT background worry the e-privacy risks what about casual person? I do not think all people need to know much about e-privacy risks and security measures as it is too early now. It is not enough at all. The promotion is also very little. No one in Oman is talking about e-privacy security. It is not enough. Up to today a lot of educated people are not aware of online security risks what about the generic citizen. <strong>Awareness</strong> efforts are mainly marketing which started since last 3 years. They are very rarely talked about privacy and security. <strong>Awareness</strong> efforts are no adequate and not covering the security risks. ITA is not yet ready for such. Up to now government is not offering many e-services. ITA is not talking about the risks and they are concentrating right now more on the promotion aspects. Government think that if they start talking about risks then they might avoid people from using the services. I think such <strong>awareness</strong> should not be forgotten thus it should be gradually given to the people. Not at all.</td>
</tr>
</tbody>
</table>
Not enough. It is not comprehensive to cover online security. IT people mostly careless. Awareness is not up to the level. Mostly it is marketing. In term of security, we are far behind. Awareness is OK despite that it is at its beginning.

No, there is no enough awareness. In order to get citizens to use e-government services awareness efforts should be increased.

Not at all. Oman should utilize the TV as a tool to reach people. Omanis know only very high level about the project.

<table>
<thead>
<tr>
<th>Usefulness=save time, efforts, ...,cost</th>
<th>Expected usefulness of E-government services:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes, it is important and essential to:</td>
</tr>
<tr>
<td></td>
<td>To save time, cost, and efforts.</td>
</tr>
<tr>
<td></td>
<td>Reduce paper work.</td>
</tr>
<tr>
<td>Success=Actual success=adoption</td>
<td>More government transparency.</td>
</tr>
<tr>
<td></td>
<td>It is 24/7 government services.</td>
</tr>
<tr>
<td>Intention = will use = will not use</td>
<td>Unify government units to have common goal.</td>
</tr>
<tr>
<td></td>
<td>To go with global trends.</td>
</tr>
<tr>
<td></td>
<td>Better interaction.</td>
</tr>
<tr>
<td></td>
<td>More efficiency.</td>
</tr>
<tr>
<td></td>
<td>Reduce many social problems such as roads traffic.</td>
</tr>
<tr>
<td></td>
<td>More land coverage of government services.</td>
</tr>
</tbody>
</table>

Yes, it will succeed whenever it saves citizens time, efforts, and cost. However, it has taken so long. Omanis will not mind give personal information to the government thus they will hesitate to share their financial data.

Yes I do, I do not know of any obstacles.

Yes sure, The success thus will take time; it will take up 5 years.

The informative e-government will succeed, however, transactional will take longer as it will be faced with integration and standardization requirement across all stake holders.

Yes, Oman is not the only country implementing such project. To avoid the failing factors, Oman should learn from others. The human factor is the main obstacle; the government should encourage the younger citizen while promoting such project.

Yes it will be successful if not on full it will be in part. Things usually take time for the people to acknowledge the change. The main obstacle is the people mentality to adopt the change.
It is too early to judge as I am away from the project. Yes it is slow but it is due to low demand. People will use it further as they get its benefits. We expect the success as long as the efforts are sincere. Further cooperation between government units will increase the success chances. That depends on the society’s awareness and readiness. If not it will not. The more people use it successfully the more success will be. It will be but gradually. I don’t trust e-services despite my professional skills. It depends on the awareness efforts and the comprehensiveness and the strength of the infrastructure to get the citizen e-government access and availability. I think this will take time. Yes it will but it will take 5-10 years. Nowadays the infrastructure is weak, very few e-services sites, and no e-payment gateways. Not in the near future and it will take not less than 5 years. ITA has no power for ITA to force other government units to have their services online. Whenever there are sincere efforts the project will be successful. To reach the people, the project is in need for a lot of awareness. I think it will be successful. The promotion is also minimal. The main obstacle is the weak infrastructure to meet the requirements for easy access. Awareness is also weak. It is possible within 3-5 years and it will no be 100%. The main obstacle is weak infrastructure and access affordability. The digital divide is still wide. Yes, I think so as the people will make it succussed in order for them to conduct easier interaction with government. Main obstacles are the people mentalities, poor infrastructure, and limited awareness.

Social Norms

They might influence my decision only whenever I am ready to be convinced and persuaded that such service is secured and it is of importance to me. Family members and friends usually practice some pressure on my general decisions and using E-government services in more specific. They think E-services are not completely safe yet. In third world countries usually there is no much of personal privacy so it would make no difference whenever we use E-government services. No one can influence my decision.
Appendix E: Interviewees’ feedback vs. research constructs
### Interviewees’ feedback vs. research constructs

<table>
<thead>
<tr>
<th>Related construct and others</th>
<th>Participants’ responses</th>
<th>Extracted finding</th>
</tr>
</thead>
</table>
| E-privacy risk concerns     | **Interviewee 1:** Not much, but I think it is loosing control on financial data and personal data as well. Personal Information is not as important as of financial type. It is really depends on the amount of personal exchanged. What always concern me is that some sites are no trustworthy. E-services are not yet so popular, however, I saw about a program on e-privacy fraud.  
  **Interviewee 2:** I think risks might come from hackers who are able to abuse/ use our personal data with no permission. Online data misuse and data tracking and mining.  
  **Interviewee 3:** I am with an excellent IT background worry the e-privacy risks what about casual person?  
  **Interviewee 4:** Yes, I am concern about some body misusing mu personal data. I am mostly concern of somebody using my data for political or criminal misuse where I am innocent. Yes, people will not give anything if any risk is anticipated; or at least they will delay taking any favorite action. Yes negatively.  
  **Interviewee 5:** Concerns do exist. Privacy risks are there and we have to protect it as much as possible. The concerns should not be and obstacle. Internet is as using airplanes for flying people use to worry that flying from place to another will spread and transmit viruses and diseases, but today who can life without flying someday. | In Oman not many people know about E-privacy concerns as they did not use online services very much. The lack on E-privacy concerns knowledge is not only among casual citizens but among educated people too and technicians too. Interviewee 19 described the status as “Up to today a lot of educated people are not aware of online security risks what about the generic citizen.” Interviewee 3 also stated “I am with an excellent IT background worry the e-privacy risks what about casual person?” Interviewee 10 also viewed “because of lack knowledge a lot of people do not think it is of importance. People still only worries of losing their online money.” However, those who know about it vary on defining the term. Interviewee 2 described the privacy risks as “I think risks might hackers who are able to abuse/ use our personal data with no permission. Online data misuse and data tracking and mining.” Where Interviewee 6 defined it as “Misusing my personal data.” Interviewee 7 further elaborated on defining privacy risks by stating “Unauthorized or not as agreed authorized use of my personal data, such use might affect people financially or socially. Parents nowadays have to watch their children not only while they...
**Interviewee 7:** Unauthorized or not as agreed authorized use of my personal data, such use might affect people financially or socially. Parents nowadays have to watch their children not only while they are out of the house but even when they are in the house with them. It is a disaster for IT illiterate parents. All online personal data concern me as there is a chance for other people to abuse them. In both what concern me is my children, family, and financial data. I am after efficiency and commitment.

**Interviewee 8:** I do not advise anybody to put their personal data online. Those people who are not entitled to know my data they should not, and those who should know they should do what is required only. The government should make use of a third party experience in order to fully protect the data.

**Interviewee 9:** We hear and read about it. I think it is whenever someone abuse somebody’s e-privacy. I heard about it elsewhere but not in Oman.

**Interviewee 10:** Because of lack knowledge a lot of people do not think it is of importance. People still only worries of losing their online money.

**Interviewee 11:** My main concern is that my data might be used by a third party without any authorization. The concern is always there as no 100% protection exists.

are out of the house but even when they are in the house with them. It is a disaster for IT illiterate parents. All online personal data concern me as there is a chance for other people to abuse them. In both what concern me is my children, family, and financial data. I am after efficiency and commitment.” Others were not sure about its meaning thus they guess almost right. Interviewee 9 stated “We hear and read about it. I think it is whenever someone abuse somebody’s e-privacy. I heard about it elsewhere but not in Oman.”

Omanis do concern of E-privacy risks however their fear is from the unknown. Such fears were caused due to lack of knowledge and awareness. Interviewee 4 described his concerns as “Yes, I am concern about some body misusing mu personal data. I am mostly concern of somebody using my data for political or criminal misuse where I am innocent. Yes, people will not give anything if any risk is anticipated; or at least they will delay taking any favorite action.” Interviewee 5 confirmed such concern by noting “Concerns do exist. Privacy risks are there and we have to protect it as much as possible. The concerns should not be and obstacle. Internet is as using airplanes for flying people use to worry that flying from place to another will spread and transmit viruses and diseases, but today who can life without flying
Privacy concern depends on the data’s details. If the citizen found that his data might be at danger, negative reaction might be taken. My credit card is considered to be very personal along with the family details. The second party should not use but according to the agree purpose.

Interviewee 19: Up to today a lot of educated people are not aware of online security risks what about the generic citizen. someday.” Interviewee 11 expressed the concern as “My main concern is that my data might be used by a third party without any authorization. The concern is always there as no 100% protection exists. Privacy concern depends on the data’s details. If the citizen found that his data might be at danger, negative reaction might be taken. My credit card is considered to be very personal along with the family details. The second party should not use but according to the agree purpose.”

Therefore, Omanis mostly think that by avoiding the use will help them of being protected. Interviewee 8 recommended such by stating “I do not advise anybody to put their personal data online.” Such decision was viewed by this study to be the most dangerous case to E-government project success.
Appendix F: Participants’ responses summary
<table>
<thead>
<tr>
<th>Interview Q. key words</th>
<th>Replay summary</th>
<th>Interview Q. key words</th>
<th>Replay summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Experience and background</td>
<td>All p have Internet Experience for 3-10 yeas</td>
<td>E-privacy concerns.</td>
<td>(13) Type of concerns</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(6) Personal information</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(4) Financial information</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(3) Both</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(4) Do not have concerns</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Reasons of concerns</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(3) Un-trustworthy employees working for these sites</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(2) Hackers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(4) Unauthorized use.</td>
</tr>
<tr>
<td>E-service experience and background</td>
<td>Most participants were Average – Expert</td>
<td>E-privacy impact on the success of e-government services.</td>
<td>(5) Depends on the awareness and regulations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(2) Depends on sites’ reputations and usefulness.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(12) Yes with negative results.</td>
</tr>
<tr>
<td>Is e-government essential to Oman?</td>
<td>All responses were ‘Yes’</td>
<td>E-privacy concerns influence on the use of e-government services.</td>
<td>(8) Negative influence.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(11) I will use it despite the concern but with higher precaution.</td>
</tr>
<tr>
<td>Social norms influence</td>
<td>(2) They might influence my decision.</td>
<td>E-commerce trustworthiness versa e-government services</td>
<td>(9) I trust e-government services more</td>
</tr>
<tr>
<td></td>
<td>(1) No one can influence my decision</td>
<td></td>
<td>(3) I trust e-commerce services more</td>
</tr>
<tr>
<td></td>
<td>(16) No comments.</td>
<td></td>
<td>(1) I trust both</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(6) I distrust both</td>
</tr>
<tr>
<td>E-government awareness efforts in Oman (adequacy/comprehensiveness)?</td>
<td>(17) Awareness is very low and not comprehensive.</td>
<td>Impact of citizen’s e-privacy concerns awareness in using e-government services.</td>
<td>(3) No impact</td>
</tr>
<tr>
<td></td>
<td>(2) ITA is doing an appreciated effort.</td>
<td></td>
<td>(7) Marginal impact as they don’t know the concerns</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(9) High impact</td>
</tr>
<tr>
<td>E-government services project chance of success</td>
<td>(10) Yes, it will be successful.</td>
<td>E-privacy concerns.</td>
<td>(13) Have concerns</td>
</tr>
<tr>
<td></td>
<td>(1) Oman should learn from others.</td>
<td></td>
<td>(6) Personal information</td>
</tr>
<tr>
<td></td>
<td>(1) It is too early to judge</td>
<td></td>
<td>(4) Financial information</td>
</tr>
<tr>
<td></td>
<td>(7) It will fail if not enough truly sincere efforts.</td>
<td></td>
<td>(3) Both</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(4) Do not have concerns</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Types of concerns</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(3) Distrust employees working for these sites</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(2) Hackers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(4) Unauthorized use.</td>
<td></td>
</tr>
<tr>
<td>How much do you know about e-privacy concerns? Is it of important to protect it?</td>
<td>Know</td>
<td>E-privacy protection practice</td>
<td>(11) Some how yes</td>
</tr>
<tr>
<td></td>
<td>(6) Not much.</td>
<td></td>
<td>(4) Not at all</td>
</tr>
<tr>
<td></td>
<td>(9) I know about the risks.</td>
<td></td>
<td>(4) I don’t use it to protect myself</td>
</tr>
<tr>
<td></td>
<td>(1) I know about it but not in Oman Importance</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(6) It is only important when relate to my money.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(2) Not important.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Omani e-services and e-privacy readiness | (9) Not ready  
(5) Some are ready  
(1) Ready  
(3) Not sure | Future intention with respect to use of e-government services | (7) If useful, I will use  
(7) If trustworthy, I will use  
(5) It will be compulsory |
|---|---|---|---|
| Trustworthiness of e-government services in Oman | (4) Yes it will be  
(4) I hope so  
(10) If it meets protection/usefulness standards  
(1) It is not | | |
Appendix G: Interview data vs. research hypotheses
# Interview data vs. research hypotheses

<table>
<thead>
<tr>
<th>Research related hypothesis</th>
<th>Interview participants’ feedback summary</th>
<th>Interview data Vs. hypothesis</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.1 Social norms will positively influence perceived usefulness.</td>
<td>Interviewee 3: “They might influence my decision only whenever I am ready to be convinced and persuaded that such service is secured and it is of importance to me.” Interviewee 4: “Family members and friends usually practice some pressure on my general decisions and using e-government services in more specific. They think e-services are not completely safe yet. In third world countries usually there is no much of personal privacy so it would make no difference whenever we use e-government services.”</td>
<td>Not enough evidence</td>
</tr>
<tr>
<td>H.2 Social norms will positively influence trustworthiness of e-government services.</td>
<td>Interviewee 18: “I will trust at the beginning until something wrong happen to me or to someone I know. I learned from this interview and I started to be more concerned.”</td>
<td>Doesn’t agree</td>
</tr>
<tr>
<td>H.3 Prior e-services experience will positively influence trustworthiness of e-government services.</td>
<td>Interviewee 1: “My major precaution is not using it very much. Also, I do not save any personal data in a computer that is linked to the Internet.” Interviewee 3: “I have an excellent IT background, and I worry about the e-privacy risks. What about a casual person?”</td>
<td>Doesn’t agree</td>
</tr>
<tr>
<td>H.4 E-privacy risk concerns will negatively influence perceived usefulness.</td>
<td>Interviewee 4: “Yes it is important and essential despite all anticipated risks.” Interviewee 7: “… I will not take chances if I don’t have to and I will think twice before taking any related decision.” Interviewee 19: “I expect e-government will help me utilize its usefulness but I will pay special attention to e-privacy risk.” Interviewee 11: “My main concern is that my data might be used by a third party without any authorization. The concern is always there as no 100% protection exists. Privacy concern depends on the data’s details. If the citizen found that his data might be in danger, negative reaction might be taken. My credit card is considered to be very personal along with the family details. The second party should not use except according to the agree purpose.”</td>
<td>Doesn’t agree</td>
</tr>
</tbody>
</table>
| H.5 E-privacy risk concerns will negatively influence trustworthiness of e-government services. | Interviewee 1: “… What always concern me is that some sites are not trustworthy.”
Interviewee 13: “I do take precaution actions when I deal with e-commerce sites. I do not use sites that I doubt their security measures. I search for online privacy policies before using the site.”
Interviewee 10: “I don’t give true information; however, I will have to give true complete information to the government. I am a very conservative user and I don’t give my personal data to an Internet connected computer.”
Interviewee 5: “I am going to use e-government services whenever they exist despite all concerns and risks.” | Agree |
| H.6 Perceived e-privacy protection will positively influence perceived usefulness. | Interviewee 7 “It is essential. Government services are 24/7 and that enhances our daily interaction with the government. However the data should be highly protected from unauthorized use”
Interviewee 11 “If the citizen found that his data might be at a danger, negative reaction might be taken and he would avoid using it despite its expected usefulness”.
Interviewee 13 “If the government gives me security grantees, I would use it otherwise it would be not very useful to me”. | Agree |
| H.7 Perceived e-privacy protection will positively influence trustworthiness of e-government services. | Interviewee 2: “I will trust e-services whenever I feel they are protected, if the other way around I will not give my personal data.”
Interviewee 5: “We are not the first so we would learn from others. It can be enhanced through awareness and e-law will help too. In my opinion privacy trust has relation to: Ethics, cultures and regulations, government transparency will no doubt increase the trust. Sites should maintain high level of commitment. The government has the required commitment however the people working for it need more skill sharpening and training. Online law will increase e-government services trustworthiness.”
Interviewee 6: “If obligatory this is out of question. Otherwise it will depend on management and behavioural factors. The government related employees should be ethically controlled. All involved parties should have a high level of commitment.”
Interviewee 7: “Those people who are not entitled to know my data they should not, and those who should know they should do what is required only. The government should make use of a | Agree |
third party experience in order to fully protect the data.”

Interviewee 9: “To increase the trust the government needs to have more e-privacy security assurance, online policies, and the right regulations and laws. E-commerce sites are more trustworthy as they much worry about their reputation except whenever the government sites worry in the same way.”

Interviewee 10:” I do not think it is 100%. Government employees should respect the people’s personal data. The citizens should know their rights and obligations.”

Interviewee 12: “Whenever Oman upper portal is in operation, I will trust it. I will expect e-government services are highly secured.”

Interviewee 13: “…If the government applies all protection efforts and it grants security, it would be very trusted. However, if not it will not be trusted. The government should do all it takes to relax the citizens’ concerns and hurry up in having the online regulations and laws.”

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| H.8 E-privacy awareness will negatively influence the level of e-privacy risk concerns. | Interviewee 15: “… awareness is needed to enhance usability trust. I will use it if it is easy and useful.”
Interviewee 6:”… Government think that if they start talking about risks then they might stop people from using the services. I think such awareness should not be forgotten. It should be gradually given to the people.”
Interviewee 16: “No, there is not enough awareness. In order to get citizens to use e-government services awareness efforts should be increased.” |
|   | Agree |
| H.9 Perceived trustworthiness of e-government services will positively influence perceived usefulness. | Interviewee 3 “It would be of a greater usefulness if it is a trustworthy. It will save me time, efforts, money however I would need to trust the site first” (3:D2).
Interviewee 12 “because I expect it to be trustworthy, I will enjoy the services usefulness and I will use Oman upper portal.” (12:D2). |
|   | Agree |
| H.10 Perceived trustworthiness of e-government services will positively influence the intention to use e-government services. | Interviewee 1: “Omanis will not mind giving personal information to the government but they will hesitate to share their financial data.
Interviewee 6: I usually trust the thing until something wrong happens.”
Interviewee 15: “I will use the service. The government already has my data. E-regulations should be in place.
I will always use whenever there are e-government sites that are secure. Security and awareness are needed to enhance usability trust. I will use it if it is easy and useful.” |
|   | Agree |
| H.11 Perceived usefulness will positively influence intention to use e-government services. | Interview 19: “Yes I will use it if I have no choice. I will not take chances if I don’t have to and I will think twice before taking any related decision.”  
Interviewee 3: “I will use e-government. I am a gambler and risk taker as long as there are benefits expected.”  
Interviewee 7: “Yes I will use it if I have no choice. I will not take chances if I don’t have to and I will think twice before taking any related decision.”  
Interviewee 8: “Despite any risk expectation, I will use it because I think it would be more efficient.”  
Interviewee 17: “I am one of those who have a high level of enthusiasm. I am looking forward to using e-services for their usefulness despite any expected risks.”  
Interviewee 15: “I will use the service. The government already has my data. E-regulations should be in place. I will always use e-government sites that are secure. Security and awareness are needed to enhance usability trust. I will use it if it is easy and useful.” | Agree |
Appendix H: List of measurement items
<table>
<thead>
<tr>
<th>Item name</th>
<th>Item label</th>
<th>Item description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use1</td>
<td>Perceived usefulness of e-government services 1</td>
<td>E-government sites would provide valuable services for me.</td>
</tr>
<tr>
<td>Use2</td>
<td>Perceived usefulness of e-government services 2</td>
<td>The content of the e-government sites would be useful to me.</td>
</tr>
<tr>
<td>Use3</td>
<td>Perceived usefulness of e-government services 3</td>
<td>E-government services would enhance my effectiveness in searching for government information.</td>
</tr>
<tr>
<td>Use4</td>
<td>Perceived usefulness of e-government services 4</td>
<td>Using e-government services would improve my government transaction performance.</td>
</tr>
<tr>
<td>Use5</td>
<td>Perceived usefulness of e-government services 5</td>
<td>Using e-government services would increase my overall productivity.</td>
</tr>
<tr>
<td>Use6</td>
<td>Perceived usefulness of e-government services 6</td>
<td>Using e-government services would enhance my government transactions effectiveness.</td>
</tr>
<tr>
<td>S_nor1</td>
<td>Social norms1</td>
<td>My family think I should use the e-government services.</td>
</tr>
<tr>
<td>S_nor2</td>
<td>Social norms2</td>
<td>My colleagues think I should use the e-government services.</td>
</tr>
<tr>
<td>S_nor3</td>
<td>Social norms3</td>
<td>My friends think I should use the e-government services.</td>
</tr>
<tr>
<td>S_nor4</td>
<td>Social norms4</td>
<td>People I knew think that using the e-government services is a good idea.</td>
</tr>
<tr>
<td>Exper1</td>
<td>Prior e-service experience1</td>
<td>I have conducted e-services on the Internet.</td>
</tr>
<tr>
<td>Exper2</td>
<td>Prior e-service experience2</td>
<td>I have used the Internet to find information about services and products.</td>
</tr>
<tr>
<td>Exper3</td>
<td>Prior e-service experience3</td>
<td>I have paid for products or services on the Internet using e-services sites.</td>
</tr>
<tr>
<td>Exper4</td>
<td>Prior e-service experience4</td>
<td>Many times I have requested further information about certain products or services on the Internet.</td>
</tr>
<tr>
<td>Exper5</td>
<td>Prior e-service experience5</td>
<td>So many times I have paid utilities’ bills using electronic medium like the Internet.</td>
</tr>
<tr>
<td>Con1</td>
<td>E-privacy risk concerns1</td>
<td>I’m concerned that e-government sites will collect too much personal information about me.</td>
</tr>
<tr>
<td>Con2</td>
<td>E-privacy risk concerns2</td>
<td>It would bother me if e-government sites ask for personal information.</td>
</tr>
<tr>
<td>------</td>
<td>------------------------</td>
<td>---------------------------------------------------------------------</td>
</tr>
<tr>
<td>Con3</td>
<td>E-privacy risk concerns3</td>
<td>E-government sites should not use personal information for any purpose unless it has been authorized by individuals who provided the information.</td>
</tr>
<tr>
<td>Con4</td>
<td>E-privacy risk concerns4</td>
<td>If e-government sites ask me for personal information, I would think twice before providing it.</td>
</tr>
<tr>
<td>Con5</td>
<td>E-privacy risk concerns5</td>
<td>E-government sites should take more steps to make sure that the personal information in their files is accurate.</td>
</tr>
<tr>
<td>Con6</td>
<td>E-privacy risk concerns6</td>
<td>E-government sites should have better procedures to correct errors in personal information.</td>
</tr>
<tr>
<td>Con7</td>
<td>E-privacy risk concerns7</td>
<td>E-government sites should never share personal information with other government units unless it has been authorized by the individuals who provided the information.</td>
</tr>
<tr>
<td>Con8</td>
<td>E-privacy risk concerns8</td>
<td>E-government sites should take more steps to make sure that unauthorized people cannot access personal information in their computers.</td>
</tr>
<tr>
<td>Aware1</td>
<td>E-privacy awareness1</td>
<td>I am aware of the e-government project in Oman.</td>
</tr>
<tr>
<td>Aware2</td>
<td>E-privacy awareness2</td>
<td>I am aware of e-privacy risks.</td>
</tr>
<tr>
<td>Aware3</td>
<td>E-privacy awareness3</td>
<td>I am aware how to protect my e-privacy.</td>
</tr>
<tr>
<td>Aware4</td>
<td>E-privacy awareness4</td>
<td>I am not aware about what information e-government sites could collect about me.</td>
</tr>
<tr>
<td>Protec1</td>
<td>Perceived e-privacy protection1</td>
<td>E-government sites will not use my personal information for any purpose unless I authorize them to do so.</td>
</tr>
<tr>
<td>Protec2</td>
<td>Perceived e-privacy protection2</td>
<td>E-government sites will devote time and effort to preventing unauthorized access to my personal information.</td>
</tr>
<tr>
<td>Protec3</td>
<td>Perceived e-privacy protection3</td>
<td>E-government sites databases that contain my personal information are well protected from unauthorized access.</td>
</tr>
<tr>
<td>Protec4</td>
<td>Perceived e-privacy protection4</td>
<td>E-government sites will really remove my personal information when I request them to do so.</td>
</tr>
<tr>
<td>Protec5</td>
<td>Perceived e-privacy protection5</td>
<td>I feel that e-government sites will make enough efforts to keep my personal information and credit card information out of the hands of unauthorized individuals.</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Trust1</td>
<td>Perceived trustworthiness of e-government services1</td>
<td>In general, the Internet is now a robust and safe environment for e-government services transaction.</td>
</tr>
<tr>
<td>Trust2</td>
<td>Perceived trustworthiness of e-government services 2</td>
<td>The Internet has enough safeguards to make me feel comfortable using it to interact with the government.</td>
</tr>
<tr>
<td>Trust3</td>
<td>Perceived trustworthiness of e-government services 3</td>
<td>I think Omani e-government sites will be trustworthy.</td>
</tr>
<tr>
<td>Trust4</td>
<td>Perceived trustworthiness of e-government services 4</td>
<td>Omani e-government sites will have more to lose than to gain by not delivering on their promises.</td>
</tr>
<tr>
<td>Trust5</td>
<td>Perceived trustworthiness of e-government services 5</td>
<td>The behaviour of Omani e-government's sites will meet my expectations</td>
</tr>
<tr>
<td>Trust6</td>
<td>Perceived trustworthiness of e-government services 6</td>
<td>Omani e-government sites will keep citizens’ best interests in mind.</td>
</tr>
<tr>
<td>Intent1</td>
<td>Intention to use e-government services1</td>
<td>I would use the e-government services to gather governmental information.</td>
</tr>
<tr>
<td>Intent2</td>
<td>Intention to use e-government services2</td>
<td>I would use e-government services provided over the web.</td>
</tr>
<tr>
<td>Intent3</td>
<td>Intention to use e-government services3</td>
<td>Interacting with the government over the web is something that I would do</td>
</tr>
<tr>
<td>Intent4</td>
<td>Intention to use e-government services4</td>
<td>After visiting e-government sites, I would be willing to provide personal information to these sites.</td>
</tr>
<tr>
<td>Intent5</td>
<td>Intention to use e-government services5</td>
<td>Acknowledging all the measures of e-privacy protection on the e-government sites, I would be willing to continue using them.</td>
</tr>
</tbody>
</table>
References


Jaeger, P. T., & Thompson, K. M. (2004). Social information behavior and the democratic process: information poverty, normative behavior, and electronic


http://www.worldatlas.com/webimage/countrys/asia/om.htm


Every reasonable effort has been made to acknowledge the owners of copyright material. I would be pleased to hear from any copyright owner who has been omitted or incorrectly acknowledged.
Publications arising from this research

The following refereed publications have resulted directly from the research reported in this thesis:
