2018

An investigation into trust and security in the mandatory and imposed use of financial ICTs upon older people

David Michael Cook
Edith Cowan University

Edith Cowan University

Copyright Warning

You may print or download ONE copy of this document for the purpose of your own research or study.

The University does not authorize you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site.

You are reminded of the following:

- Copyright owners are entitled to take legal action against persons who infringe their copyright.

- A reproduction of material that is protected by copyright may be a copyright infringement. Where the reproduction of such material is done without attribution of authorship, with false attribution of authorship or the authorship is treated in a derogatory manner, this may be a breach of the author's moral rights contained in Part IX of the Copyright Act 1968 (Cth).

- Courts have the power to impose a wide range of civil and criminal sanctions for infringement of copyright, infringement of moral rights and other offences under the Copyright Act 1968 (Cth). Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.

An investigation into trust and security in the mandatory and imposed use

of financial ICTs upon older people

This thesis is presented for the degree of

Doctor of Philosophy

David Michael Cook

Edith Cowan University

School of Science

2018

USE OF THESIS

The Use of Thesis statement is not included in this version of the thesis.

ABSTRACT

Care needs to be taken to reduce the number of people who are fearful and mistrustful of using ICT where that usage is forced upon them without choice or alternative. The growing incidence of mandatory and imposed online systems can result in confusion, misuse, fear, and rejection by people with only rudimentary ICT skills. A cohort where a high percentage of such people occur is older people, defined in this study as people over the age of 60 Examples of compulsory ICT interactions include some banks limiting bank statement access through online rather than paper-based options. Other examples include the purchase of theatre or sports events tickets through ticketing systems that require an online transaction to take place.

Increasingly, people are living beyond the normal retiring age. As the older cohort increases in size and in overall global population percentage, the problem of forced technology usage affects technology acceptance, technology trust, and technology rejection. People care about ICT systems where reduced trusted acceptance of technology reduces the advantages of digital health care, the perceived security of banking and shopping, and the autonomy of ICT-driven lifestyle choices.

This study aims to solve one of the puzzles of ICT-driven change, where older people can show trepidation towards using technology. By understanding the drivers that influence the choices older people make in relation to ICT systems, it may be possible to introduce a much higher level of trusted acceptance in ICT systems. Although many people adopt ICTs into their lives, many older people face difficulty in using technology when it is forced upon them. This study aims to understand the connection between how choice (or lack of choice) can lead to the rejection or resistance towards ICT usage. Older people sometimes opt towards practices that place themselves at risk of financial or informational disadvantage.

This study used a qualitative approach to understanding the factors that influenced the trusted acceptance, trepidation, and in some cases rejection of ICT usage by interviewing a sample of older people. Participants were asked to consider a wide range of ICT-usage scenarios and to describe their intentions. The study focussed on circumstances where ICT usage fell under either mandatory, imposed, or voluntary conditions in order to compare user behaviour. Settings included a range of technology-reliant states that examined IT security, volition and choice, aging, trusted acceptance, and technology

adoption. Participants were interviewed to discover and sort the conditions (whether singly or in combination) under which the expectation of ICT acceptance was in some way altered, diminished, or prevented.

This research found that older people made poor decisions when the choice to use a technology was replaced with a mandatory or strongly imposed pathway. Mandatory ICT usage across the broad area of financial transactions brought about widespread fear and distrust of online technology usage. The results revealed that many older people not only find these innovations daunting and confronting, but they also have difficulty placing their trust in ICT systems and applications that have become mandatory. In normative conditions, increased ICT acceptance and ICT usage is expected. When ICTs are mandatory in their usage, acceptance is replaced with compulsory procedure. This does not mean that mandatory things cannot be accepted, but rather that older people will accept the need to use a technology according to their perception of what is necessary for their daily and routine interactions.

This study showed that voluntary ICT usages including choices increase informed decision-making, security of online financial interactions, and trusted reliance upon ICTs. Choice in ICT usage carries greater trust than mandatory, obligated, or heavily imposed ICTs. The study revealed that mandatory ICT systems can create perceptions of fear, mistrust and uncertainty. In situations where a mandatory ICT system becomes the normative method of transaction, a strong risk to the trusted acceptance of a technology is not merely the lack of ICT-based choice, but also the inability to gain reassurance or secondary confirmation through either face to face or telephone-based communication. Trust in not just the usage, but the implied secure usage of mandated and imposed ICTs, is problematic for older people.

This study revealed the significance of mandated ICT systems that limit choices for people, because older humans more readily validate and associate their trust in new innovations when they can access various different professional, technical, peer-based, social and popular opinions. The research also showed that older people are fearful and less trusting in mandatory and imposed systems because they have less financial resilience, and less opportunity to bounce back from loss and disadvantage brought about by digital and online interactions. Older people were worried and reluctant to accept technology at first glance because they knew that they had spent more time than others in a pre-internet,

pre-digital environment, and their seminal life experiences are correspondingly less technology-related. The results showed that many older people preferred human communication and interaction rather than communicating, buying, paying, and trusting in purely digital, ICT-based experiences. This demonstrated a gap in the trust and security of digital systems, and the need to address those ICTs that impose and mandate instruments and procedures for daily life.

Specifically this study looked at what could reduce unsafe and insecure banking practices by understanding the role of choice in the trusted usage of ICT systems. This study is significant because it shows that older people make financial and social, decisions under reactionary, insecure, and under-informed conditions as a result of a gap in terms of trust security and choice. On the one hand older people develop trust towards a new innovation based on accumulated human discussion, information and reputation. On the other hand older people hold the perception that online systems offer reduced choices.

This study led to the development of a model for trusted technology choice (TTCM). It differs from traditional acceptance and diffusion thinking, by having outputs as either ICT acceptance or ICT rejection. It diverges from diffusion and technology acceptance models (TAM), because technology acceptance is not regarded as a foregone conclusion. Instead, it places a very high value upon choice and volition, trust, security and human interaction. The TTCM model, together with a framework for identifying volition barriers, provides a different set of criteria for understanding the needs of older people and their meaningful interactions with new innovation and ICTs.

The practical applications for using such a model directly impact upon financial and social stability for older people. Where choices are either removed or limited due to ICT usage, older citizens are unfairly disadvantaged. A model that accurately predicts the trusted usage of ICT innovations can have a widespread effect on the implementation of large-scale public and private systems where the trusted acceptance (or rejection) of each system has on flow impact on financial, health, and other critical services that include the growing population of older people.

DECLARATION

I certify that this thesis does not, to the best of my knowledge and belief:

 (i) Incorporate without acknowledgment any material previously submitted for a degree or diploma in any institution of higher education;

 (ii) Contain any material previously published or written by another person except where due reference is made in the text; or

 (iii) Contain any defamatory material.

I will also grant permission for the Library of Edith Cowan University to make duplicate copies of my thesis as required.

Signature ....

Date .... 23 / 4 / 2018 ....

ACKNOWLEDGEMENTS

Undertaking a project of the size and scale of a doctoral investigation is an activity that takes enormous time and effort. It is both a challenge and a torment, and it is best done without additional barriers, save for the social needs that all people should maintain. To that end, this study has been engaged with the knowledge that its completion through sickness and health and in competition with full-time work and commitment represents a significant achievement. It has been done to the exclusion of other things, other people, and other opportunities.

I acknowledge the people who have assisted me to complete and to offer what is hopefully seen as a useful contribution. To my wife Rebecca, my family and my friends, I thank you for your patience and your understanding. To my colleagues and peers, I also offer gratitude. To my supervisors I give you my thanks. In particular, I thank Professor Trish Williams and Dr Martin Masek for their efforts in guiding me through the task. Your feedback and guidance is always welcome.

GLOSSARY OF TERMS

The following terms and acronyms are used throughout this thesis. The Information Communication and Technology sector uses many abbreviations and acronyms as efficient descriptors. Where possible the use of such abbreviations is maintained throughout this document.

AARP	American Association of Retired Persons
ABC	Australian Broadcasting Corporation
ABS	Australian Bureau of Statistics
ACCAN	Australian Communications Consumer Action Network
ACMA	Australian Communications and Media Authority
ADL	Activity of Daily Living
AHRC	Australian Human Rights Commission
ANPEA	Australian Network for the Prevention of Elder Abuse
ANZ	The Australian and New Zealand Bank
APSC	Australian Public Service Commission
APWG	Anti-Phishing Working Group
AR	Action Research
ASIC	Australian Securities and Investments Commission
AT	Activity Theory
ATM	Automatic Teller Machine
CAPTCHA	Completely Automated Public Turing Test to tell Computers and Humans Apart
CBA	The Commonwealth Bank of Australia
CDT	Cognitive Dissonance Theory
CFA	Country Fire Authority
CV	Curriculum Vitae
DHA	Department of Health and Ageing
DHS	Department of Human Services
FBI	Federal Bureau of Investigation

HSBC	Hong Kong and Shanghai Banking Corporation
ICT	Information, Communications and Technology
IDT	Innovations Diffusion Theory
KMV	Key Mediating Variables
NBN	National Broadband Network
OFT	Office of Fair Trading
PU	Perceived Usefulness
PEOU	Perceived Ease of Use
SCOT	Social Construction of Technology
SMH	Sydney Morning Herald
SN	Subjective Norms
SSM	Soft Systems Methodology
STAM	Seniors Technology Acceptance Model
TAM	Technology Acceptance Model
TPB	Theory of Planned Behaviour
TR	Technology Readiness (Model)
TRA	Theory of Reasoned Activity
TRI	Technology Readiness Index
TTF	Task Technology Fit
UNDP	United Nations Development Program
UTAUT	Unified Theory of Acceptance and Use of Technology

TABLE OF CONTENTS

1   CHAPTER 1   INTRODUCTION

"Molly receives notification from her bank that she will no longer receive bank statements via postal mail, and that she must go online to the bank's website, enter her account number and password, and access the downloadable statements from the online facility. Molly is a senior citizen aged 75 who has no knowledge of how to use a computer, nor does she own one. She visits the bank and asks for a statement at the counter. Instead of printing a statement, the banking teller points to a computer in the foyer of the bank – and tells her that she may print out her own statement "at no cost" using the bank's computer and printer. Molly then leaves the bank, without a statement, and unable to ascertain the state of her finances. She subsequently turns to her cleaning carer, the only other person she regularly sees, and asks her for assistance. The cleaning aid takes her account number and password and promises to print out a statement from her computer at home, and to get a copy to Molly. Molly thus finds herself trusting someone that she doesn't know very well with the confidential access to her account, yet at the same time cannot establish a trusted relationship with her own bank. She knows that she is open to being taken advantage of, but feels that she has little choice. She does not trust online systems, and does not understand what is required to use them with any proficiency".

The above scenario of Molly is typical of the ICT-related burdens that face older people. The requirements to undertake online banking can be either mandated (as in the example) or imposed (where the cost of a statement in the post becomes prohibitive in comparison to a free download). In the above scenario, even though Molly uses the system through an older person's carer, the usage clearly does not imply trust of the system. Instead it infers the risky combination of reliance upon a carer, and the reluctant continued usage of a technology because Molly may feel that she has no viable alternative. The result is an assumption that the corresponding carer's usage of an IT system is necessary if she wishes to read a bank statement.

Several online tasks are sufficiently effectual to the wider community that their former physical counterparts are no longer palatable, or are culturally and environmentally objectionable. For example,

paperless systems gain favour over printed records where large numbers of in-print documents raise questions of environmental concern, storage space, and financial cost (Fairchild, 2003; Kane, 1981).

The social, environmental, and financial burden of paper record keeping is challenged by the concept and application of virtual and electronic storage of key documents (Belanger & Hiller, 2006: Chan et al., 2010; Suh & Han, 2002). Paperless systems are (in the eyes of older people) a partial change only, because older people know that they can print out a digital record onto paper with great ease. Printers have been in existence for hundreds of years, so older people may not feel that they have swapped from paper to paperless, because in reality they are often engaging in activities that store both the printed and the digital record (Cresci, Yarandi, and Morrell, 2010). Older people trust printers and place great trust in a printed copy of a record (Kerai, Wood, Martin, 2014). It forms a tangible thing that can be held in one's hand and physically placed or stored (Mannan and van Oorschot, 2008). Printed records on paper are psychologically difficult things to destroy (Laukkanen, Sinkkonen, and Laukkanen, 2009). Photo albums become prized family possessions that retain image integrity whereas digitally pictures can be easily altered, manipulated, and redistributed (van Dijck, 2008; Keightley and Pickering, 2014).

The challenge becomes more complicated in the context of older people who resist change from trusted systems that deliver security and easily accessible information management (Oxendine, Borgida, Sullivan, & Jackson, 2003; Wu, Ozok, Gurses, & Wei, 2009). Notable cases involve partially mandated elements of ICT usage. For example, whilst many banks offer online banking as optional, the choice requires the mandatory requirement to accept cookies before any transactions can be completed. Since most older people don't understand cookies in the context of web data, partially mandated usage such as agreeing to accept cookies requires older people to make uninformed decisions about ICT usage in the face of uncertainty and financial risk (Pavlou, 2003).

Technology and innovation is swiftly spreading around the globe, however its spread is uneven, and its acceptance is "at best" sparse, intermittent and irregular (Heather, Ryan and Teague, 2010; Yi and Okamoto, 2013). When Everett Rogers first launched his thoughts on Diffusion Innovation in 1962 he told of the manner in which a South American public health service attempted to convince Peruvian

villagers of the benefits of boiling their drinking water. The local health operative, described in Rogers' work, comprehensively failed in her efforts to convince twenty-one village housewives to boil water before drinking it. (Rogers 1962). This is a useful parallel to understanding the issues in convincing older people to take up the benefits of technology and ICT innovation.

All new ideas and concepts have a variety of differing speeds of uptake, from the early adopters through to the later adopters, then the "laggards", and in some cases those who reject the new idea entirely (Rogers 2002; Banyte and Salikaite, 2015). Whilst the terms early and late adopters are self-explanatory, this research also makes reference to laggards who deliberately take time to consider, and in many cases reject, new technology and innovations. Terms are sometimes popularised and the term laggards has been associated with laziness and idleness, however the term laggards in this research should be taken to describe those people who make a conscious decision to either delay, think about, or discard the usage of new ICTs. Laggards are an important subset of older ICT users since they make deliberative and purposeful choices in relation to the diffusion of new technology. The diffusion of ideas is itself a phenomenon, and the manner in which ICT has taken global acceptance with such rapid speed and ubiquity is often taken as a sign that it has acceptance at all levels.

However, acceptance of technology is also bound by caution (McCoy, Galletta, King, 2007; McLean, 2011). Systems that are critical, that are used in the treatment of the sick (Botella, Etchemendy, Castilla, Banos, Garcia-Palacios, Quero, Alcaniz and Lozano, 2009), or the deployment of highly sophisticated weaponry are expected to operate flawlessly simply because they are digital and not human (Clothier, Greer, Greer, & Mehta, 2015). Digital elections are entirely possible, enabling genuine democratic voting to take place, yet they are not commonplace in society (Halderman and Teague, 2015; Alvarez and Hall, 2003). In other words, for certain systems if we are to trust technology, then it must be perfect (Belanger, and Carter, 2008). Society seems to accepts the human flaws (Dekker 2014; Lonsdale, 2004), but is less accepting of the flaws of a digital system (Lou, Li, Zhang and Shim, 2010; Lee, 2009).

Whilst we trust a human bank teller to give us the right number of banknotes in a withdrawal, we form a different trust in the automatic teller machine (ATM) that dispenses our banknotes through its cash cartridge (Lee, 2009; Gefen, 2000; Kim and Benbaset, 2006). One is a human trust based on

mutual understanding between customer and teller, and strengthened by a combination of expectations, fears, obligations and responsibilities (McKnight and Chervany, 2001), and the other is a one-sided affair, characterised by our acceptance of crypto-processors and our ability to remember a four number personal identification number (Li, Li and Winsborough, 2009). The human qualities of face to face trust are cooperative and collaborative (Almenarez, Marin, Diaz, and Sanchez, 2006). The technical qualities of an ATM are technically reliable, yet humanly non collaborative (Li et al, 2009). An ATM does not count the right number of notes because it wants to keep its job, nor does it recognise the customer, but rather it acknowledges the presentation of a magnetic strip card and a correctly entered four-digit Personal Identification Number.

For humanity, however, the emergence of a mistake can cause humans to question trust, to look for a human reason that explains the mistrust-worthy behaviour (Belanger and Carter, 2008; Pew Research, 2014). Notable issues are always characterised with a range of explanations such as "human error", "cultural differences", and "connectivity" (Rogers 1962). All can be used with the reliance upon reasoning that has gained our trust because we develop an understanding of the various characteristics that fit the experience. Technology Acceptance Methodologies (TAMs) argue that we get used to our experiences (Venkatesh, Morris, Davis and Davis, 2008), however usage does not necessarily equate to understanding. Such errors also draw out elements of scepticism, cynicism, disbelief, and mistrust (Alston, 2014; Chang, McAllister, McCaslin, 2015; Lewicki, McAllister, and Bies, 1998).

The point here is to emphasize that usage is not always an indicator of trust. Caution and risk are therefore useful descriptors to help frame the issue of technical versus human differentiation. For older people, technology has often appeared to be in favour of a younger generation, or the young at heart (Caprani, Doyle, O'Grady, Gurrin, O'Connor, Caufield and O'Hare, 2012; Obi, Ishmatova and Iwasaki, 2013; Cortes, Barrue, Martinez, Urdiales, Campana. Annicchiarico and Caltagirone 2010). Older people tend to be more accepting of a new proposition that required a judgement about the trust of a person than a judgement of a technology (Mollenkopf, 2004; Minkler and Holstein, 2008). As people grow older they add to their life experiences in becoming more astute in the assessment of their fellow humans (Pew Research Center, 2014). By contrast, as people grow older they become less

connected with physical human interactions as technologies disrupt their customary networks (Cotton, Anderson, and McCullough, 2012).

This study examines the difference between "use" and "trusted use", as well as the difference between "acceptance" and trusted acceptance". Thus a definition of trusted use and trusted acceptance is where the use of a technology is undertaken by a person with the person's belief that they freely choose to use that technology with the expectation that the technology will perform according to its intended purpose. This definition is explained in Renaud and van Biljon, (2008) as a person's attitude to acceptance or rejection of a technology. The definition is derived from Silverstone and Haddon's (1996) five stage process for product adoption. In addition there is a difference between acceptance in the short term and adoption in the long term. Short term acceptance (usage) does not necessarily translate to trusted usage until such time as the user chooses to adopt a technology. That choice implies trusted usage; if it is made freely and based on the user's own sense of utility.

Older people actively seek to use what they perceive as their better-developed human judgement and expertise wherever possible (Wright, 2009), often in preference to judgements using technology because they trust their own instincts above a preordained set of technical constituents (McLean, 2011). Digital systems have less in common with tolder people than with younger people (Mordini, Wright, Wadhwa, De Hert, Mantovani, Thestrup, Van Steedham, Amico, and Vater, 2009). There is a generational and cultural gap that is well marked (Minkler and Holstein, 2008), and strongly defended by a global cohort of older persons who achieved their accomplishments largely without the help of the digital age (Meyer and Mollenkopf, 2003).

That generational positioning forms one of the explanations for the questioning that older people have towards the approach to digital systems and the promise of betterment of life through ICT ubiquity (Wright, 2008; McLean, 2011). Whilst there are older people who embrace new technology and new innovations with energy, there are also a very large number of late or non-adopters (Rozanova, 2010). Often they are older people who refute the need to change for the sake of change alone (McLean, 2011). Older people place a notionally richer and more complex set of humanly-connected criteria upon trust than the typical proposition of usage and therefore acceptance (Hammel, 2004). They make decisions much more closely with their human interactions, and they are more cautious about digital

systems, and the people behind those digital systems (Tinker, McCreadie, Stuchbury, Turner-Smith, Cowan, Bialokoz, Lansley, Bright, Flanagan, Goodacre, and Holmans, 2004). As people grow older their decisions, their trust, and their acceptance of technology incorporate more skills, more life experiences, and more understanding (McLean, 2011).

1.1 Older users and Technology

This research is grounded by two emergent trends fronting humanity: widespread population aging and the exponential diffusion of technology (Charness, 2004; Cutler, 2011). Information Communication and Technology (ICT) systems are ubiquitous, and afford interactions with a multiplicity of e-services, ranging from social, financial, communal, governmental and organisational services (Fano & Gershman, 2002; Phang et al., 2006: Phang, Yan, Sutanto, & Kankanhalli, 2005: Weiser, 1991). ICT usage amongst older people has risen rapidly in line with the overall progression of ICT usage and new technology uptake (Peacock & Kunemund, 2007). Older people have a less technologically advanced understanding of ICTs than those from younger age brackets (Charness & Boot, 2009; Maniom, 2011). This paucity of ICT development is potentially dangerous and harmful because whilst early usage of ICTs developed alongside physical, face to face communication systems, ICTs are now promulgated as independent mainstream systems of interaction (Czaja & Lee, 2007; Peacock & Kunemund, 2007; Selwyn, Gorard, Fyrlong, & Madden, 2003). Society (including older people) is now expected to use ICTs to engage in communications, financial operations, (typically banking), and as the main source for information discovery (Fisk, Rogers, Charness, Czaja, & Sharit, 2009).

This study considers the use of technology by older people specifically of the age 60 years and over. This age limit is chosen for this study because it represents both an established retirement milestone as well as a social milestone where the majority of Australian older people are no longer working. The research in this study considers mandatory, imposed and voluntary usage of technology, but is less restricted by the imposed and mandated technology that is often incorporated into working

life. Thus the results of this study should more naturally allow for the issues of trusted technology to be more accurately evaluated, with the data obtained relating to the individual technology usage of older people rather than the more imposed technology usages that can sometimes relate to working life. This milestone is useful for an Australian study because it incorporates the age at which there are changes in a person's working/retiring identity, their autonomy, and their finaiincial stability (Baltes and Smith, 2003).

Older people face complications in undertaking routine actions where they depend on the Internet and the ability to operate some form of Internet-connected device (Barker, 2012; Norris, 2001; Weatherall & White, 2000; Yang, Whitefield, & Boehme, 2007). These difficulties range from technical issues such as ICT literacy (Charness & Boot, 2009; Cook, Szewczyk, & Sansurooah, 2011b; McKay, 2009) to social issues such as trust and confidence (Ellis & Allaire, 1999; Horrigan, 2008), and can include financial concerns such as affordability, confidentiality and security (Benamati & Serva, 2007; Cook, Szewczyk, & Sansurooah, 2011a; Gan, Clemes, Limsombunchai, & Weng, 2006; Yeow, Yuen, & Tong, 2008). These elements in combination are symptomatic of a well established problem. That problem is in the form of ICT usage by older people without the necessary experience, acceptance, finance, capability and understanding to carry out routinely imposed digital interactions (Kane and West 2005; McLean, 2011). Growth in aging populations, technology confidence and the digital divide fuel social, cultural and financial stress on both governments and individuals whilst large sections of the community are constrained, marginalised or isolated from the information society (Agarwal, Animesh, & Prasad, 2009: Niehaves & Plattfaut, 2010). Trust is required at social, cultural and financial levels.

ICT usage falls into segments of use that are either mandated, non-mandated, or a combination of mandated and non-mandated interactions (Gupta, Dasgupta, & Gupta, 2008; Venkatesh, Morris, Davis, & Davis, 2003). ICT Usage can be segmented as mandated, imposed, or voluntary.

Mandated ICT usage is where there is no alternative other than to use ICT to complete a transaction. Examples of mandated usage include the purchase of concert tickets that are only for sale online, or government departments that advertise employment insisting on a CV or resume that is sent via email. There are many mandated ICT processes that are taken for granted by younger generations but are less accessible to older people (McLean, 2011).

Imposed ICT usage appears in the form of ICT processes where there is both an ICT approach as well as a face to face approach, but that the ICT version is overwhelmingly less difficult, less expensive, and more anticipated than a face to face exchange. Examples of imposed ICT usage can include payment systems for utilities, banking accounts where the statements are available online rather than through the postal mail, and health rebates where the processing system is deliberately structured to convenience the online transaction before the face to face one (Tinker et al, 2004; Fealy, Donnelly, Bergin, Treacy and Phelan, 2012).

Voluntary systems offer an ICT pathway as well as a human face to face option. Voluntary ICT opportunities appear fair and non-discriminatory; however the weight of community expectation and customer experience is often skewed towards a digital transaction (McHugh, 2003; Werner, Carlson, Jordan-Marsh, and Clark, 2011). Examples include older people queuing at banks and post offices to make financial payment transactions.

There is considerable overlap between mandatory, imposed, and voluntary segments. Older people report confusion over their ability to grasp which ICT interactions are required and which may be undertaken by other means (Horrigan, 2008). They subsequently take advice regarding ICT interactions from a range of individual, commercial, and in some cases disreputable sources, many of whom have a vested interest in seeing older people undertake increased ICT usage (Bitterman & Shalev, 2004; Pew, 2014). Hence, the usage of ICTs fosters the perception of requirement rather than choice for an increasing number of activities including but not limited to financial, utility-based, and health-related digital transactions. Older people regularly cite that they are forced to use computers (McMillan, Avery, & Macias, 2008; Redding, Eisenman, & Rugulo, 1998), and that they need to trust others with online functions (Keat & Mohan, 2004) because they are uncertain of some aspects of ICT usage (Morris, Goodman, & Brading, 2007; Morris & Venkatesh, 2000).

1.2 The Problem

Imposed technology interactions that demand usage do not equate to a form of trusted acceptance. Instead they equate to an enacted (but untrusted) acceptance of what becomes someone

else's requirement. In some cases an imposed ICT interaction can lead to technology rejection. Various segments of the older person's cohort form decisions about what and who to trust based upon different criteria to younger generations. Technology and its acceptance play a major role in this differentiation. Requests to trust technology that present in the forms of online banking, bill paying, and government services are deliberated against a range of variables including whether technologies are either mandated or imposed. Restricted and removed options for human interaction when dealing with financial transactions is unacceptable to some older people and uncomfortable to others.

Older people, particularly those who are novices in the use of ICTs, are highly vulnerable to financial and informational risk from exploitation using technology and systems that they do not understand. Older people who are technology stragglers are increasingly suffering from identity theft, credit card fraud, reputational damage, social engineering, phishing, and ransom-ware (Schneier, 2008; Frumento, and Freschi, 2016; Tzezana, 2017). Their usage of ICT is rapidly being extended into a range of imposed and mandated interactions that place them at greater risk and likelihood of being compromised. This indicates that this group of people may be unable to make important decisions using ICTs because they are unable to ascertain which forms of ICT and its associated usage can be trusted.

Globally the number of older people is increasing as people live longer (ACMA, 2009; Murray, Barber, Foreman, Ozgoren et al, 2015). Worldwide ICT diffusion and acceptance are responsible for the implementation of a great many mandated and imposed digital systems. Finances and information are controlled using ICTs that require user acceptance and user trust. However not all systems should be accepted, and not all usage should be mandated. Imposed and mandated use of ICTs can be used but not trusted, meaning some people feel coerced to engage in the use of ICTs under conditions where their finances, their security, and their significant lifestyle decisions are based on uncertain and diffident foundations. The need to cater for marginalised cohorts, such as older people who are ICT novices, requires that trust in ICT choices must be investigated.

1.3   Significance

The study considers the choices (or lack thereof) made by older people when asked to trust mandated or imposed ICT technology. The study examined whether there is a significant relationship between the choice to use ICTs and the trusted usage of ICTs. The findings of this study will redound to the benefit of society considering that trusted ICT usage plays an important role in the financial, social, and communal wellbeing of older people. The growth in the number of people living to older ages justifies the need for more effective acceptance of technologies by older cohorts to deliver financial security, better access to government services, and greater inclusion to activities that are disseminated by means of ICTs. Thus financial agencies, government organisations, and community organisations in general will be able to more effectively gain the trusted inclusion of older people. The findings of this study will assist in the improvement of new ICT systems and pathways where trusted acceptance by older people has previously been diminished.

The study aims to explain the effect that mandatory technology usage can have upon older people, in order to mitigate insecure online behaviour, to reduce under-informed decision-making, and to forecast insecure behaviour that arises from the rejection or resistance to mandatory and imposed ICT technologies. The implications on the reduced acceptance of ICTs in education, health, governance and stability are vast (Chesters, Ryan, & Sinning, 2013; McKay, 2009; Norris, 2001). Examples include reduced usage of human computer interaction (HCI) in digital voting, government funded health programs, local, state and federal government ICT training programs, and online responses to government surveys, online safety information, and government funded mobile device applications. The study advances the HCI community's understanding of the way in which older adults react to technologies when presented with usage requirements that are characterised by limitations in terms of choice. In some instances older people are prevented from choosing between ICT and non-ICT alternatives, and this study shows how different choice–reduced situations might be managed so as to be acceptable to older people. By gaining increased trusted acceptance of the delivery of ICT systems in training, health, finance and government, older people can improve personal, local and national uptake of costly government funded programs. An example of a significant improvement is in the information and training of online security for older people. Training is provided through government

created online web portals, yet older people who are forced to use an ICT system before they know enough to trust an ICT system remain hesitant and wary to "go online" (Australian Government, 2013; Australian Government, 2015). This study shows that where older people are able to choose between learning about ICT security in online or in face to face delivery, or in a written form on paper rather than online, there is a much greater level of readiness to learn about ICT security. This study also advances the field by demonstrating how situations where ICT usage is either mandated or imposed can be better managed so as to provide a trusted form of acceptance that is acceptable to older people. As choices are removed and online security portals seemingly become the expected and imposed pathway to become educated about ICT security, there are greater numbers of older people who feel coerced. Some people are imposed and forced to the point that they either give up being serious because they feel trying to find the online information is pointless, or they lose overall trust in ICTs and give up at the earliest point in time to use ICTs.

Similarly, the benefit of increased uptake of the Australian Government program to join to an ICT-driven health record system is significant, yet reduced by older people who do not trust ICT record keeping through MyGov, PCEHR, or My Health Record offerings (Partel, 2015). Such examples are significant because they show instances where the trusted acceptance of an ICT can assist to bridge knowledge gaps, and improve social, economic, and health conditions. This study showed that some people were unwilling to use digital online systems that stored their health records. Their reluctance came about because they held little or no confidence that their records were secure from others because they were stored digitally rather than in a paper form, and that such systems were sophisticated to the point where older people were incapable of feeling that they could make determinations about the trustworthiness of a digital pathway and access system for medical records. Thus, governments and health agencies that examine the means by which health records may be stored with reference to trusted choices will be able to better guide older users towards ICT-based information and data systems.

The transition from "over the counter" and "face to face" banking to online systems requires users to change from the security of personal recognition, written signature verification, and human behaviour to online passwords and multi-factor authentication systems. Users who are uncertain about online banking revert to several unsatisfactory practices (Pew, 2003; Chakraborthy, Bagchi-Sen, Rao,

and Upadhyaya, 2012). This affects many older people (Maab, 2011; Gamble, Boyle, Yu, and Bennett, 2014). This study shows that some people felt they were forced to abandon their older transactional practices in banks where they had trust in a written signature, and where they knew some of the staff, and where staff knew them. These people placed a greater level of trust in older forms of multi-factor authentication (signature, passbook, and known to staff) than in newer forms of multi-factor authentication such as passwords, pin numbers, mobile phone verification and email verification.

1.3.1 Misplaced Trust

In cases where users reject the idea of carrying out online banking they may instead feel forced to trust someone else who has enough technology skill and capability to carry out transactions for them. The significance of this behaviour is that older people (particularly those who live in relative isolation and are often alone) find themselves forced to choose someone who may not be suitable. Such instances include examples of financial elder abuse, where a helper, carer, or acquaintance is given online access, and subsequently takes advantage of the situation, by stealing portions of money, or by taking control of an older person's financial assets. The reduction of financial elder abuse through greater ICT uptake can greatly reduce the reliance upon social welfare (and the burden on government) needed to subsidise older people who would otherwise have retained their retirement savings and would have retained financial, housing, and lifestyle independence (Stanger, 2015). Financial institutions will be able to draw from the findings of this study to better understand the required balance between customer ICT capabilities and imposed online access systems that can be trusted by older people with limited skill and appetite to use ICTs.

1.3.2 Forced Acceptance

Some older people realise that their banking is being conducted through online means, and contemplate whether to accept the use of digital technology. Since many older people have a limited understanding of online technology usage and in the act of making financial transactions, they may conduct themselves in an unsafe manner, on home computers with little or no security, and which are extremely vulnerable to attack from malware, social engineering and targeted attacks. Mandated use

of technology also denies people of their autonomy. Modern society acknowledges the rights of individuals to make their own choices to the exclusion of interference from others (Renaud and Van Biljon, 2008). It is one of the cornerstones of contemporary ethics that people should be able to make decisions through one's own independent thinking (Sensen, 2013).

The findings of this study demonstrate the considerable need for financial institutions to redress the home user's usage of online banking systems. Such findings provide the impetus for financial institutions to provide online banking access that contributes to a home-user environment that provides a greater level of security within a trusted set of systems that provide trust and confidence in the daily interaction with banking systems for older people.

The findings of this study can assist financial institutions (and their associated vendors and supporters) to reconsider the importance of ICT usage that can be trusted because it does not depend upon imposition or coercion for it to be repeatedly used for ongoing transactions. Where banking institutions offer online statements for free, but tell customers that there are fees for each page of a posted bank statement, older people feel obliged to change to online banking. Whilst the change is not mandatory, they will feel that the change is being imposed upon them, with limited choice. The significance of this is that some older people have small amounts of available money and unlike younger generations, have retired and are living under conditions where their income is unlikely to increase. Banking offers such as free online statements are open to interpretation by older people as threats, and resultant behaviour is that older people move to online banking without the necessary training, hardware, or capabilities to safely practice online financial transactions. In many cases this leads to vulnerability from email and spam correspondence, phishing attacks, and phone-related social engineering. If older people cannot access statement information, then they are at risk of financial fraud, and are vulnerable to a range of financial abuses (Chang et al., 2015; McLean, 2011; Pew, 2014).

1.3.3   Technology Rejection

In many instances, older people have discussed their lack of trust with other peers, and as a result they may make the decision to reject technology altogether for their financial transactions. The significance of this is that many older people then revert to unsafe personal practices, attempting to

store life savings in the form of cash or other instruments rather than accepting the bank's online systems for their day to day transactions. Thus the findings of this study reveal the factors that underpin the rejection of technology by older people seeking to remain anchored to non-ICT financial interactions.

1.3.4 Flow-on effects and the Influence of Financial online acceptance or rejection

Since older people place an enormous stock in their financial accessibility, their trust (or lack, misdirection, or imposed behaviour) has a flow–on effect to other important online interactions. This is significant because it can influence the decision-making of older people against important transformational systems such as online Census collections and E-voting. Thoser older people who do not trust an online banking system are likely to transfer that lack of trust into other systems. This study's findings can give significant direction to solving the more general benefit of trusted ICT usage for important events such as online voting, referenda, and digital transfer and storage of statistical data from census collections.

1.3.5 Choice and Perceptions of Trust

Older people do not need to have been robbed to form an opinion about the trust of ICTs. By focussing on the way older people perceive government services and facilities (including public transport, emergency services and community announcements), greater levels of information sharing (trusted usage) can be obtained. Information systems that offer choices in terms of information dissemination and information sharing are rewarded with perceived trust from older people. An example of this is where a community announcement is made online with reference to further information at a specified URL, but also includes information sheets as PDFs that can be saved and printed, as well as options for phone contacts to call, and physical addresses where older people can attend in person to find out more information.

The research shows a correlation between the difficulty in trusting new and emerging forms of ICT usage whilst retaining a set of existing safe and trusted options that may use little or no digital technology. This is significant because as ICTs become more and more commonplace, the time and

cost to society of accounting for an older cohort that holds perceptions of mistrust will reduce ICT efficiencies and increase program costs for a range of financial, health, and social services. The research aimed to predict usage and rejection decisions through the addition of mandatory, imposed and voluntary criteria. A new model of technology acceptance and adoption for older citizens can assist novice older people to make more informed decisions about ICT innovations that rely on trust under mandated and imposed conditions. Providers of critical technology in areas such as banking, health, and social services will be able to draw on the research to improve the level of trust in ICTs by older people. The research addressed the trust and security concerns of ICT stragglers who are generationally disadvantaged towards technology innovation. A specific focus of this study aimed to assist older people who feel compelled to accede to mandated and imposed ICT usage without sufficient regard to their safety and security. By understanding the key determinants that influence novice older ICT users, stragglers and late adopters can survive vulnerable and risk-based ICT impositions that limit financial and information-based choices.

If society adopts a "one size fits all" approach to technology acceptance, then a growing older population is likely to become more disenfranchised from the use of ICTs. Mandatory ICT systems, along with heavily imposed systems, might be the cause of technology rejection, and as a result bring about obstructive and uncooperative interactions by older technology users. This would impact across a range of technology solutions for older people, ranging from assistive technology in the home, to democratic rights in the form of voting. This study aims to provide clarity to the contested issues surrounding ICT-related trust, rights, and mandated systems. If this research is not conducted, it is possible that generation after generation of older people will find themselves exposed to greater risk, as they occupy the middle ground between experienced users and novice users.

1.4 Hypothesis and Research Question

Based upon the established problem of trust and mandatory technology practices, this study clarifies the key elements of choice and trust in secure ICT usage. The study is predicated on the consideration of the following proposition.

The hypothesis:

That mandated and imposed interactions with ICTs by older users, reduces their trust in ICTs, which leads to insecure financial behaviour through imposed choices, reduced freedoms, technology rejections and greater risk of online cyber-crime.

Notes about the Research Question

In order to test the above hypotheses this research question asks:

What affects the way older people make informed decisions about trust in ICT innovations that involve imposed or mandated online financial interactions?

Models that predict the behaviour of those accepting technology have so far failed to allow for three main features that isolate novice older citizens. The first is that models thus far do not adequately allow for the specific variables pertaining to older people who are late adopters in ICT understanding. The second is that technology acceptance models do not fully appreciate (and give weighting to) imposed and mandated ICT usage. The third is that the overwhelming majority of technology acceptance models do not adequately allow for the possibility of ICT rejection (on an equal basis to acceptance). This question seeks to understand why some people trust online banking whilst others reject ICT systems in favour of face to face financial interactions.

This research highlights one of many challenges that face society as older constructs of physical data and informational transactions shift to virtual environments. Judgements and decisions about trust in physical assets and their systems are different to judgements about assets that are stored in cyber systems. For example, in 2001 an older woman might cautiously guard her cash withdrawal from a bank teller or automated teller machine (ATM). In 2015 the caution is more squarely centred on the protection of her online banking password and her at home computer security. Thus the need to understand trust and technology takes on a greater level of importance. Critical areas of technology trust require a clearer understanding of how older people will accept or reject their existence, especially in the areas of banking, finance, medical records, and personal identity. The vulnerabilities for older people lie more closely with their perceived trust of a system than with the system provider's level of

security. Both are important in the protection of financial or medical data, but without freely acquired trust, good quality security systems are at risk from poor choices made by older individuals.

This study looks at the need for more careful judgement in the execution and deployment of ICTs and their related systems that impose or mandate their usage. There is an established portion of literature that suggests that older people demonstrate usage and rejection behaviours towards mandatory ICTs more markedly than other age groups (Botella et al., 2009; Caprani et al., 2012; Chang et al., 2015). This study provides information that distinguishes between the stereotype that many older citizens will always lag behind younger generations in terms of technology (McLean, 2011), and the under-recognised impact that mandatory ICT innovations have upon the trust, acceptance, and secure usage of ICT technology (Wu, et al., 2013; Botella et al., 2009). This helps to answer how issues about mandated ICT can be generational, or whether future cohorts of older people will remain at risk of mandated and imposed technology systems.

.

1.5   Structure of the Thesis

This thesis begins by introducing the topic and giving an in-depth background to, and a critical analysis of, the problem that requires solution. It outlines that older people, whilst perhaps generally challenged by new technology and ICT-based innovations, are more specifically affected by those ICT technologies that become imposed or mandatory. The main suggestion is that trust and security of ICTs under such conditions is problematic. The thesis then formally begins with a review of the literature, presented in chapter 2 (See Figure 1).
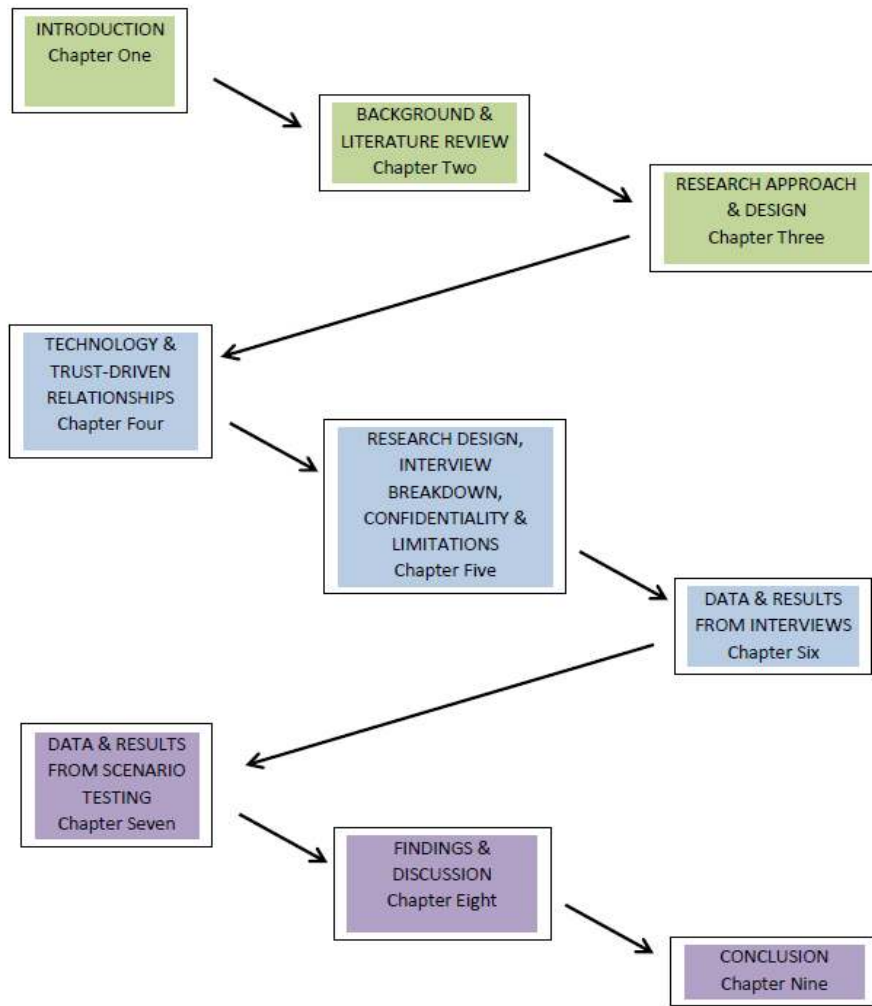
Figure 1.1 Roadmap of Doctoral Research

Chapter 2 describes the background to the study and describes the literature review which comprises of five main areas of review. The first is cyber security, the second area of review looks at volition and choice, the third area of review examined the specialist area of gerontechnology, the fourth area of review studies trust and governance, and the fifth area discusses the development of information diffusion systems, and acceptance and technology trust models.

Chapter 3 describes the research methodology and the research design. The chapter describes the methodological, ontological, and epistemological foundations for this study. It explains the choice of an Emancipatory Action Research approach and why this was chosen over other approaches. The chapter includes a consideration of both quantitative and qualitative approaches and explains how the methodology is arrived at, and how competing methodologies were considered and then excluded after

careful analysis. It shows the research structure and the methodology by examining relevant methods of conducting research on the acceptance and rejection of technology and innovation. The research methodology used for this study is described along with a rationale for the choices made in terms of sampling, data collection, data analysis, and reporting stages.

Chapter 4 explains the importance of technology and trust-driven relationships. It discusses and reflects upon a one-sided aspect that much of the literature on technology acceptance and diffusion fails to question. It discusses a misrepresentation whereby the majority of the technology acceptance literature equates acceptance with trust. This chapter explains the need to resolve a clearer understanding about technology trust, especially under imposed, coerced, and mandated conditions. It introduces the important concept of technology rejection as a viable alternative to what is sometimes automatically aligned towards technology acceptance.

The chapter presents a set of theoretical summaries that demonstrate new and different measures of trust. These outlines distinguish divergent trust-based choices that suggest alternative technology-based as well as non-technical options to older citizens. It includes an attempt at a clearer set of variables as expressed in a simple model of understanding. The key focus is to differentiate trust in terms of mandated, imposed and voluntary usage of technology. It also includes a range of cultural factors.

The chapter also reflects upon the literature and existing acceptance thinking to more deeply explain the relationship between trust and imposed and mandated technologies. In this chapter technology acceptance is considered in isolation from usage. Instead, this chapter describes the manner in which older people make choices about the normal aspects of their existence. It looks at older people in terms of their activities, their needs and their limitations. The cultural, physiological, and cognitive aspects of age are used to define trust from an older person's perspective rather than a usage perspective.

Chapter 5 explains the research design, and the interview breakdown, as well as issues of confidentiality and limitations within the research. The chapter explains the difference between the interview data and the scenario testing which forms the 5th part of the interview process.

Chapter 6 presents the results of interviews and data collections of older citizens who described their levels of trust and feelings of reliance towards technology systems. These results comprise of

responses to four interview parts that consider distinctions in types and preferences of ICT usage, descriptions of technology based trust, and system preferences, and how trusted behaviours are decided when using ICTs

Chapter 7 presents the data and analysis of the scenario testing, whereby respondents have detailed their attitudes towards a range of hypothetical scenario-based examples where trust and volition are put to the test. In order to test a range of variable issues, there are 12 scenarios where the responses are dissected so as to demonstrate key drivers for understanding what might trigger technology rejection or avoidance.

Chapter 8 examines the findings and main discussion points. It discusses the key findings in relation to the research question and clarifies the important relationship between trust, imposed ICT usage and mandatory ICT usage.

Chapter 9 presents the concluding comments for the thesis. It includes a list of recommendations based upoin the findings derived from the data in chapters 6 and 7, and the key factors as explained in chapter 8.

1.5.1   Research Roadmap

The roadmap of doctoral research shown in Figure 1.1 explains the research journey in terms of sequence and order. In combination, the chapter sequences represent a roadmap that explains how to navigate the information presented through the course of this research.

1.6   Other publications by the Researcher.

There are several publications by the researcher that inform the research presented in this inquiry. They are as follows.

Cook, D. M., Szewczyk, P., Sansurooah, K., (2011), Securing the Elderly: A Developmental Approach to Hypermedia-Based Online Information Security for Senior Novice Computer Users. *Proceedings of the 2nd International Cyber Resilience Conference*, 20 - 28, Perth, Western Australia.

Cook, D. M., Szewczyk, P., Sansurooah, K., (2011), Seniors Language Paradigms: 21st Century Jargon and the Impact on Computer Security and Financial Transactions for Senior Citizens. *Proceedings of the 9th Australian Information Security Management Conference*, 63-68, Perth, Western Australia.

Cook, D. M., Kumar, A., Unmar-Satiah, C., (2015), Loyalty cards and the problem of CAPTCHA: 2nd Tier security and usability issues for senior citizens. *The Proceedings of 13th Australian Information Security Management Conference*, 101 - 111, Perth, WA

These three papers have considered individual aspects of IT trust for older people. The first paper on securing the elderly looks at generational differences in the acceptance of information technology. It does this by considering the paucity of acceptance of cyber security mechanisms by older users of ICT technology. The second paper considers the language paradigms of older people by comparing and examining the understanding and applied knowledge of older people in their interactions with information security, and the challenges associated understanding technical terms, new language, and feeling comfortable in the trusted usage of new systems and innovations. The third paper on loyalty cards and CAPTCHA looks at the potential risks of those who donate personal and private information in exchange for commercial benefit and reward as a customer. In addition, there is a full list of the researcher's publications at the end of chapter nine. These publications draw on the more general themes of governance, security, and technology.

The next chapter discusses the background and literature review for this study. It develops the literature through the five main areas of review: cyber security, volition and choice, gerontechnology, trust and governance, and theories of technology diffusion, acceptance, and behaviour.

2 CHAPTER 2 BACKGROUND AND LITERATURE REVIEW

The purpose of this chapter is to review the literature that pertains to older people and their acceptance or rejection of information technology when it is mandated or imposed upon them. The literature focuses upon areas where the hesitation and resistance of older people to use ICTs is related to perceived risks. One such risk, that the literature refers to multiple times, is the risk of being targeted by cyber criminals. The chapter establishes the scope and nature of the literature surrounding technology choices and usage, with particular focus on older citizens and their alignment with decisions relating to technology usage, and the security of financial assets. The review is not bound within a single research discipline, but considers the issues associated with technology adoption, mandated systems, security, trust and older people.

Chapter 2 comprises of five main areas of review. The first is cyber security, where the literature examines the online vulnerabilities that are specifically relevant to older people and novice users of ICT. It specifically considers three sub-topics within cyber security of application security, information security, and end-user awareness and education. The second area of review looks at volition and choice. It considers the impact and consequences that affect decision making and behaviour when choice is removed, and where obligation, compulsory and mandatory ICT usage occurs. This explains some of the limitations held by older people using technology; however reduced usage of mandated ICTs remains inconclusive (Lawhon, 1996; Benamati and Serva, 2007). The third area of review examines the specialist area of gerontechnology, where gerontology and technology are combined to reveal challenges where the social, mental and physiological changes brought about by aging are incorporated with the challenges of technology change and ICT understanding (Bouma, Fozard, Bouwhuis, and Taipale, 2007; Manitoba Government, 2001). The fourth area of review studies trust and governance. The literature looks more closely at social governance than the clinical governance and draws from the new modes of governance literature that aligns with ubiquitous technology communication. It describes governance in a structural sense (Campbell, Carter, Hobbs and Schaupp, 2012; Marsh and Briggs, 2009; Nissenbaum, 2004), that is inclusive of international standards (Kerwer, 2005; Lichtenstein and

Williamson, 2006) and transparency (Grabner-Krauter and Faullant, 2008). The last area of the literature review discusses information diffusion systems, and examines the various theories of technology acceptance and usage (Charness and Boot, 2009; Turner, Kitchenham, Brereton, Charters, and Budgen, 2010). In cases where older people attempt to engage with ICTs, the ability to understand which variables influence decision making is critical to determining the contexts under which trust-based decisions are made (Lachs and Pillemer, 2004; Chesters, Ryan and Sinning, 2013). Technology usage, acceptance and diffusion is well described generally, but is less well described with specific reference to older users (Turner, Kitchenham, Brereton, Charters, and Budgen, 2010).

The review examines this literature in component form, examining each model and trust system in individual and specific groups of systems in order to "make sense" of their relevant features and their respective implications upon older people. The analysis of the literature also considers the literature from a synthetic form, taking elements from models in order to address those key variables that impact with greater influence upon the trust-related effects for older people.

2.1 Evolution of Technology Usage by older people

Literature about older people's interactions with ICT repeatedly highlights a fear of technology and automated banking (Marr and Prendergast 1991, Kwan 1991, Marshall and Heslop, 1987, Cruz, Laukkanen and Munoz, 2011). A fundamental study by Zeithmal and Gilly (1987) showed that older people over the age of 65 were afraid to adopt banking technologies. Nothing has changed. It showed that older people prefer to interact with human tellers rather than electronic (non-human) mechanisms. The technology fear extends beyond usage of ATMs (Xiong and Matthews, 2005; Tiong, 1999; Smither and Braun, 1994) and a common thread that runs through this literature is the desire by older people for safety and security when using online banking (Howcroft, Hamilton, and Hewer, 2002; Durkin, 2007; Laukkanen and Kiviniemi 2010; Friemel, 2014). Older people are less fearful of bank transactions where there is human contact, most commonly in the form of a bank teller (Mattila, Karjaluoto, and Pento, 2003; Peral-Peral, Arenas-Gaitan, and Ramon-Jeronimo, 2012).

The spread of technology and its trusted usage has been the subject of a wide range of examination; however there remain many unresolved and contested facets within the crossover between voluntary, imposed and mandated elements of technology uptake (Adali 2013; Hill, Betts and Gardner, 2015). Indeed, there is a large pool of peer-reviewed material that attempts to explicate why certain groups engage in ICTs more swiftly, more recurrently, or more enduringly than others (Zhou, Rau and Salvendy, 2013). There are several different theories that facilitate an explanation of how people (especially older people) might go about using and trusting ICTs (Wilkowska and Ziefle 2009).

Following the normal convention of using an ICT does not automatically imply trust of an ICT (Obi, Ishmatova, and Iwasaki, 2013). There are several variables that separate trust from usage: some are based on perceptions (Renaud and van Biljon, 2008), acuities (Singer, Baradwaj and Rugemer, 2012), and sensitivities (Patriche and Bajenaru, 2010), whilst others are influenced by mandates and obligations (Mitzner et al, 2010; Brown et al, 2002; Hill, Betts, and Gardner, 2015). Understanding how different aspects of trust explain technology choices involves some complexity insomuch as it includes technical issues, cognitive functions and social theories (Burmeister, 2010; Vroman, Arthanat, and Lysack, 2015). Trust involves belief (Lawlor, 2014; Adali, 2013). The Trust connection to technology usage is born from perspectives that reflect the strength with which one person's belief is sufficiently strong to allow that person to attempt accept a technology without firstly applying tests and investigations that might reveal flaws, defects, and problems (Hoffman, Postel-Vinay and Rosenthal, 2009).

This review of the literature reveals many theories that link usage and trust (Barber 1983; Carruthers; 2009; Chang et al, 2010; Hill et al, 2015). However, the literature does not reveal any one single theory that adequately describes the relationship between trust and usage of ICTs with sufficient clarity to explain the behaviour of older people when connecting with mandated or obligated ICT systems (Adali, 2013; Brown et al 2002; Decman, 2015). This literature examines trust and usage under five main areas of research.

2.2 Five Principal Areas of Review

This chapter focuses on a review of the literature in five areas of research. They are cyber security, volition and choice, gerontechnology, trust and governance, and technology acceptance and usage. These five areas headings were chosen because the literature consistently referred to these areas when explaining how older people interacted with ICT technologies in situations where trust became a contested issue.
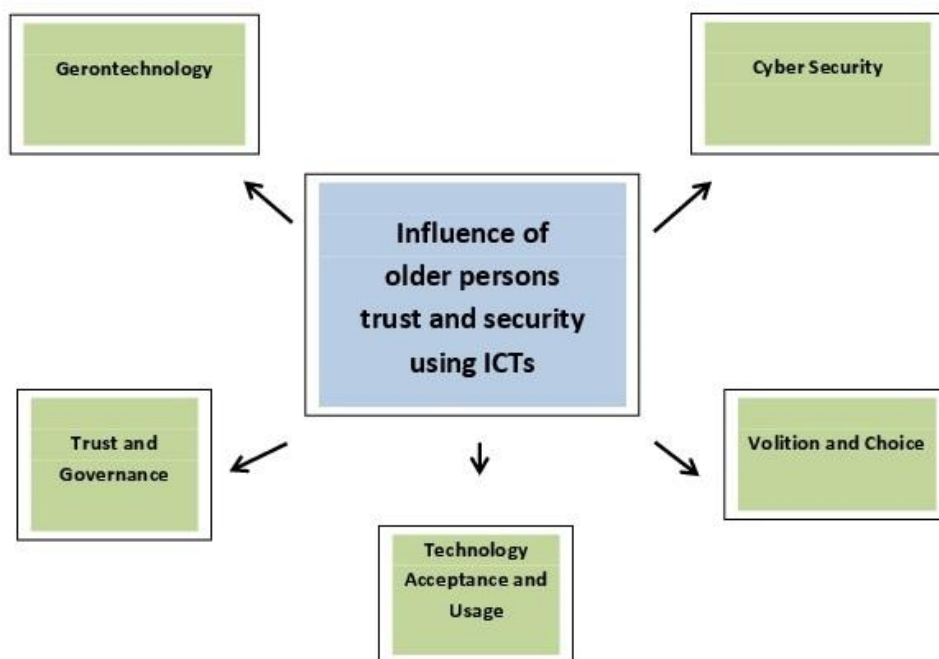
Figure 2.1 Areas of Literature Review

- **Cyber Security** relates to the body of technologies, procedures and practices intended to shield computers, networks, programs and data from attack, harm, loss, and unsanctioned access.

- Volition and Trust is an area that considers perceptions of trust based upon mandatory, imposed, or voluntary dealings.

- **Gerontechnology** is an interdisciplinary field that combines gerontology with technology to consider human activities that interact with technology interventions.

- **Trust and Governance** considers the rules and norms that drive the expectations and dynamics of those interacting with ICTs.

- **Technology Acceptance and Usage** concentrates on whether people can grow to accept an ICT innovation based upon their repeated or continued usage of a particular technology. The combination of reviewing these five areas covers the most impactful, prevalent and widespread elements that inform this study (Figure 2.1).

2.3 Cyber Security

In broad terms cyber security covers the protection of information systems from theft or damage to the hardware, the software, and the information on them, as well as the users of those information systems. It also covers the identification and mitigation of interruption and misdirection to any services they provide. In specific terms this literature focuses upon six sub-areas of cyber security:

- Online ICT Security

- Social Engineering

- Phishing

- Malware: Trojans and Keyloggers

- Advance Fee Scams

- Anti-Virus and Protection

This literature describes the conditions under which security vulnerabilities are targeted by criminals to exploit the cohort of older people (Sylvester, 2004; Choo, 2011; Kritzinger and Von Solms, 2010). The most often discussed is that of exploitation of older people using phishing (Carlson, 2006; Rengamani, Upadhyaya, Rao, and Kumaraguru, 2010; Arfi and Agarwal, 2013). Application security describes the use of software, hardware, and procedures that are used to protect applications from external threats (Richardson, Weaver, and Zorn, 2005). The literature describes resistance and hesitation to the use of banking applications based upon difficulties with the installation and comprehension of required protection systems including antivirus programs (Mattila, Karjaluoto and Pento, 2003; Bhat, 2012; Festervand, Meinert, and Vitell, 1994; Faletti, 1985; Cymek, Burglen, and Minge, 2014). Older people exhibit reservations about the transition from physical bank customer to online self-service of banking (Zeithaml and Gilly, 1987; Campbell and Frei, 2010), citing distrust with the security of banking applications (Laforet and Li, 2005; Laukkanen, Sinkkonen, Marke, and Laukkanen, 2007; Chong, Keng-Boon, Lin, and Tan, 2010), misapprehension about their own online abilities (Lam and Lee, 2006; Benamati, 2007; Gatto and Tak, 2008), and the unhappiness of performing tasks that would

have otherwise been previously undertaken by bank employees (Mathew and Stone, 2003; Durkin, Howcroft, O'Donnell and McCartan-Quinn, 2003; Morris, Goodman, and Brading, 2007).

The information security literature that refers to the older describes reluctance and unwillingness on the part of older people to expose their private information to systems that are perceived as untrustworthy, or that are insufficiently protected to prevent private data being obtained without permission (Maab, 2011; Gerling, and Masuch, 2011). Older people are significantly vulnerable to scams and financial deception (Garg, Camp, Lorenzen-Huber, and Connelly, 2011). The literature consistently identifies issues with privacy for older citizens (Millward, 2003; Arenas-Gaitan and Peral-Peral, 2015), and in the specific ICT training required to feel proficient in the use of online technology (Morrell, Mayhorn, and Echt, 2004; Ferreira, Torres, Mealha and Veloso, 2015; Zheng, Spears, Luptak and Wilby, 2015)

The literature considered both virtual and physical understandings of ICT, providing an insight into the transitional elements between 'virtual' online interactions and "real-world" face to face engagements that are normally the preferred comfort zone for older people (Purdie and Boulton-Lewis, 2003; Xiong and Matthews, 2005; Ross and Smith, 2011; OCP, 2012; Diako, Lubbe and Klopper, 2012).

2.3.1 Online ICT Security

In 2010 in Australia, the third most recorded online activity for home internet users was either paying bills online or conducting some form of online banking activity (ABS, 2011). The literature points to a reliance by older people on regular access for financial purposes (Alsajjan and Dennis, 2010; Gu, Lee and Suh, 2009). This has brought with it a range of online security-related challenges (Lee, 2009; Lichtenstein and Williamson, 2006; Ureel and Wallace, 2013; Zheng, Spears, Luptak and Wilby, 2015).

The primary emphasis of on-line security is on banking and financial interactions (Zheng et al 2015). In business terms, financial institutions balance between conversion of as many online users as possible whilst offering trusted protection from cyber fraud, deception, and online vulnerabilities (McKnight, Choudury, & Kacmar, 2002; Singer, Baradwaj, & Regemer, 2012; Suh & Han, 2002). The

literature indicates that older citizens have deeper concerns with financial security than other age cohorts (Benamati and Serva, 2007; Alawadhi and Morris, 2009; Maab, 2011). Secondly, there is an increased appetite from older people for electronic and instant forms of communication ranging from email to contemporary social networking platforms (Duggan and Smith, 2013; Vergeer and Pelzer, 2009). This immediacy provides greater opportunities for social engineering, phishing and combinational physical/virtual deceit (Carlson, 2006; Coronges et al., 2012). Despite the obvious need for security as online financial systems become ubiquitous, the number of personal and private financially-based cyber-attacks is rapidly increasing (Australian Government, 2013; APWG, 2010; Schneier, 2008)

Older people as a cohort represent a preferential target for online predation and manipulation from both criminals and legitimate financial business concerns (Carlson, 2006; Cook et al., 2011b; Schneier, 2006). Older people have a larger number of unknowing, ICT illiterate and technology-naive members than any other significant societal grouping (Audunson, 2005; Maab, 2011; Peacock & Kunemund, 2007). They are targeted for identity theft, financial dealings, and anywhere that technology ignorance can be exploited (Australian Government, 2013). They are socially vulnerable to a range of tactics both legal and illegal (Gil & Amaro, 2010; Liao & Cheung, 2003). As a target group they represent significantly easier quarry than other groups (Bratkiewicz, 2000; Cook et al., 2011a; Grimes et al., 2010; Maab, 2011). They are largely less educated and less socialised in terms of ICT knowledge (Maab, 2011). They are often asset rich from a life-time of employment (Ogrodnik, 2007), and in combination may be vulnerable from the physical and mental inertia of old age (Gatto & Tak, 2008).

The rules and expectations by which society chooses to deliver electronic communications and technology suit an audience that is generally more socially and technically informed than is the situation for large numbers of older people (Gil & Amaro, 2010; OCP, 2012; Price and Price, 2010). "Most internet fraud has clear antecedents in telemarketing fraud. The difference is the size of the potential market, and the relative ease, low cost, and speed with which the scam can be perpetrated" (Berrelez, 2000). Telemarketing fraud has been a significant problem before the advent of internet and mobile banking (Mouallem, 2002). New iterations in more recent years extend on the same set of human vulnerabilities, but with the added combinational curiosity of ICT uncertainty (Martin, 2009). Internet

consumer fraud in the 21st century threatens older people using all of the social engineering elements that have been crafted for years (Bratkiewicz, 2000). Yet many propositions are posed on an assumption of an ICT complexity, fault, or opportunity that requires the consumer to rely on the needs of an otherwise unknown third party (Carlson, 2006; Maskaleris, 2007; Rengamani, Upadhyaya, Rao, and Kumaraguru, 2010). Based on this literature regarding online banking, bill paying, and mobile banking the research indicates two factors in regards to the targeting of older people as vulnerable to cyber-attacks. The first is the perception held by cyber criminals that older people are a relatively low risk target of choice. The second is that older people regard themselves as more vulnerable to cyber-attack. This literature supports the notion that older people might be predisposed to feel hesitant about trusting online banking.

There are five main attack vectors of online theft, fraud and corruption that repeatedly apply to older people (Interpol, 2015). They are Social Engineering, Phishing, Malware, Advanced Fee Scams and Anti-virus protection (Australian Government, 2013). There are other areas of fraud and deception, however they are much smaller in practice when measured against the older person's cohort (ACMA, 2009; AHRC, 2012; Ross & Smith, 2011). The first four are particularly effective when applied by criminals to older people (AHRC, 2012).

2.3.2   Social Engineering

"The greatest threat many older Americans face is not a criminal with a gun, but a telemarketer armed with a deceptive rap" (Bratkiewicz, 2000). The contemporary equivalent facing older Australian citizens comes in the form of combinational telemarketing/computer scams such as the Microsoft scam (ACMA, 2012; Microsoft 2015). This scam has been repeatedly aimed at older people who are uncertain about the security of their own home computer and choose to accept the technical advice of an unsolicited caller claiming to be an official technician (Chawki, 2009; Harley, Grooten, Burn, & Johnston, 2012). The scam has many forms and variations, but the central objective is to convince the consumer of a fault that the technician can fix over the phone by convincing the computer owner to give remote access to their machine (Scamwatch, 2011; Whitman & Mattord, 2010). The scammer then solicits a fee in order to "restore" the machine to working order (APWG, 2010). The literature indicates

that whilst this scam has been repeatedly deployed for over six years the frequency of its recurrence suggests that there are still sufficiently large numbers of people who fall victim to the trap such that its use is continued and ongoing (ACMA, 2012).

Social Engineering has three main vectors for initiating misplaced trust: scarcity, fear, and authority (Workman, 2008). Scarcity is a reactance tactic. It works on the theory that some people will react impulsively and without thinking some elements through. It is a known sales technique that affects people of all ages. It is the least effective of the three main social engineering tactics. The key objective of social engineering is to sell trust (Gao and Kim, 2007; Mitnick and Simon 2002). Fear and authority can be used together or separately to gain trust (Wang and Emurian, 2005; Workman 2008). Older people who share a common fear of being vulnerable to an online attack or deception are susceptible to placing trust in someone who pretends to exhibit similar feelings (Yakov, Shankar, Sultan, and Urban, 2005).

In many cases this leads to poor decisions and interactions with free software that can include malicious programs such as key-logger Trojan horse combinations (Beldad, De Jing, and Steehouder, 2010). In other cases, a shared fear can lead to the sharing of personal information that can later be used for identity theft and other online fraud (Workman, 2008; Wang, and Emurian, 2005). Authority can be effective as a stand-alone tactic, and is often described through examples of e-Government, online utility payments, and e-Health (Beldad et al, 2010). In the same way the Milgram's famous experiment proved the effectiveness of a white lab coat in convincing people to commit perceived acts of fatal torture (Milgram, 1983), so the authority of e-Government can convince users to place trust in mandatory and imposed payment and data systems (Workman, 2008; Beldad et al, 2010). In 2013 the state government owned Country Fire Authority (CFA) was criticised for its iPhone mobile app that use Apple Maps, and gave highly inaccurate information as to the location of town sites relative to bushfires. Authorities from government organisations have the benefit of authority in online information systems, and people place trust in such systems because they perceive that an authority would be a highly reliable provider of accurate, trustworthy information (SMH, 2013).

2.3.3 Phishing

Telemarketing fraud is the predecessor for more sophisticated online attacks now known as phishing (Ramzan and Wuest, 2007; Carlson, 2006). Phishing is a criminal method of cyber-attack that combines social engineering and technical deception in order to; steal a consumer's personal identity data; take their business credentials; and to gain their computer access (Cook et al., 2011a; Price, 2010; Whitman & Mattord, 2010). These schemes use hoaxed emails referred to as spoofing (Shostack & Stewart, 2008). Social engineering is used to design emails that purport to be from legitimate businesses that trick consumers by leading them to fake websites where the consumer needs to establish their authenticity by divulging some form of access information such as a password, login, address or other private data (Coronges et al., 2012; Whitman & Mattord, 2010). The people using social engineering are commonly referred to as 'scammers', insomuch as they steal from people using trickery, deceit, deception and fraud (Schneier, 2008). They perpetrate criminal acts and are unhindered by sympathy and morals.

Having acquired private information and data that can be used to authenticate access to applications and programs, the scammer is then free to use the information in real sites in order to deploy financial asset or change access to data, often locking the consumer out of their own system in the process (Jagatic, Johnson, Jakobsson, & Menczer, 2007). The literature shows widespread use of phishing attacks globally, but indicates that there is a much more targeted proliferation of this style of attack generated towards older people. (Australian Government, 2013; Carlson, 2006). Additionally, criminals have a reduced risk in concentrating on older people, many of whom are too ashamed to report incidents of fraud (FBI, 2006).

Further, older people are highly susceptible to phishing attacks because they find it difficult to distinguish between real websites and fake ones (ASIC, 2011). Older people are often mistakenly trusting of fake websites because they identify with brand images, logos, and style features that make them believe they are on a valid site (Price, 2010; Shostack & Stewart, 2008). Small details such as fake URL addresses and small grammatical errors in content text are often overlooked by older people

who may have diminished eyesight or other accessibility-related constraints (Conway, 2014; Carlson, 2006). The result is that remote control access is exercised through either the use of "phisher-controlled" proxies to authentic websites or the theft of customer data using systems to record keystrokes (APWG, 2010). The literature demonstrates that phishing attacks have a high likelihood of success when deployed against older people (Kibby, 2005; Carlson, 2006: FBI, 2006).

2.3.4   Malware: Trojans and Keyloggers

Other more advanced attacks install malware onto consumers' machines using deception in a two stage process. The consumer will often open a file or attachment from an email, and install the scammers' own application for them (Blythe, Camp, and Garg, 2011; Jakobsson, Tsow, Shah, Blevis, and Lim, 2007). These applications can be activated remotely or independently at a later time (Shostack & Stewart, 2008). Older people who often pass "chain emails" with cartoon images to other people can inadvertently also install a key logger program that records and sends information about keystrokes used on a given machine (Thomas, 2008; FBI, 2006). The idea is to record keystrokes of logins, passwords and key financial data such as account numbers (Kibby, 2005, Fleeger and Fleeger, 2009). Older people who share chain emails or who venture to pornography sites put themselves at greater risk of malware infection and subsequent vulnerability to information loss, financial loss (Blanton, 2012), and computer corruption (Blythe, Camp, and Garg, 2011; Jakobsson, Tsow, Shah, Blevis, and Lim, 2007).

The literature suggests that Malware has been transferred to computers operated by older people Smirek, Henka, and Zimmermann, 2015; Cook, Szewczyk and Sansurooah, 2011a). In many cases the malware is embedded onto a system because of inadequate updating regimes for anti-virus, and a lack of understanding on the part of the user. The literature indicates that most key logger trojans are transferred through pornography and email with attachments that initiate upon opening (Bosler and Holt, 2009; Taylor, Caeti, Loper, Fritsch, and Liederbach, 2006). Chain letters with attachments are of specific risk to older people as they also appeal to the social engineering fear of an adverse event if they do pass the email on to "ten more friends" (Harley and Abrams, 2009).

2.3.5 Advanced Fee Scams

Advanced Fee scams operate on the premise that an older person has some beneficial outcome pending which is awaiting some form of confirmation (Martin, 2009; Maskaleris, 2007). In the case of some Nigerian scam emails, the promise of millions of dollars to be transferred to an account is waiting on bank account details or verification (Blanton, 2012). Often a small amount of money is requested from the older person to commence the confirmation of transfer. This in turn can evolve into a second request for money and the ruse continues until the consumer realises that they have been deceived, or they run out of money. Similar advanced fee scams operate using the bait of a lottery win, or a free trip (ACMA, 2009). In each case, the consumer is required to send a comparatively small amount in what is referred to as an advance fee (Gamble, Boyle, Yu, and Bennett, 2014). The money is rarely recovered and the advanced fee is usually sent via a wire transfer service (such as Western Union) so that it can never be traced or returned. The literature describes the repeated inability of older people in sensing the danger of such transactions and the likelihood of fraud and deception (Blanton, 2012, Carlson, 2006).

Further, whilst online fraud and corruption can affect anybody using online services, there is overwhelming evidence that older people are a much higher risk cohort than other age groups (FBI, 2006). The 2007-2008 joint Victorian Police research project revealed that people over the age of 65 were more likely to succumb to advance fee scams such as those purporting to be lottery wins, prizes, and beneficiary funds transfers (Ross & Smith, 2011). The average loss for advance fee scams was $11500 per incident (AHRC, 2012).

2.3.6 Anti-Virus and Protection

Older users of technology have difficulty in understanding the need for antivirus protection (Furnell, Bryant, and Phippen, 2007) as well as difficulty choosing appropriate protection (Yao, 2011), and in installing antivirus software (Chakraborthy, Bagchi-Sen, Rao, and Upadhyaya, 2012). Of the various areas where security is specifically problematic for older people, there is a widespread lack of understanding with terminology, jargon and nomenclature (McKay, 2009; Obi, Ishmatova, & Iwasaki, 2013). The ICT industry uses newly introduced words and abbreviations that are either ambiguous in terms of dual meanings such as '*Spam, Trojan, Worm, Cookies*' or otherwise newly created words that

had no existence in 20th century literature or conversation such as '*Phishing*' (Cook et al., 2011b; Gatto & Tak, 2008).

Further, there are usability issues that indicate many older people are unable to fully comprehend the method of removing dangerous files from their computer, even once warned through antivirus messaging (Maab, 2011). Older users are particularly susceptible to spyware, and experience confusion in distinguishing between messages about mainstream virus protection and anti-spyware protection (Hinde, 2004, Rengamani, Upadhyaya, and Rao, 2010). The literature demonstrates that older people do not understand the changing nature of anti-virus and the need to keep updating anti-virus protection. Instead, older people hold a simplistic view of Antivirus as a static, once off expense that once undertaken should offer sufficient protection.

2.4 Volition and Choice

From a cognitive science perspective, the capacity for voluntary action is considered an essential human characteristic (Haggard, 2008). It is the key element in human behaviour whereupon people consciously intend to act (or not act), and that they can choose to act, so that when describing volition, it is a description of controlling the "if, when, how, and why" of one's actions (See Figure 2).

The literature describes the difficulties that older people have with using and understanding technology, especially where the usage or the understanding is a required element. In cases where they feel obliged and locked into a particular course of action, their usage is limited. For example, older people are suspicious of imposed and automated banking practices that require customers to use online banking to access standard banking products (McKnight, Choudhury, and Kacmar, 2002; Benamati and Serva, 2007).

The literature repeatedly posits that older people are forced to consider ICT-related concerns about password integrity, privacy, and the protection of personal information (Pavlou, 2003; Rotchanakitumnuai and Speece, 2003; Eriksson, Kerem, and Nilsson, 2005; King, Ureel, Kumar and Wallace, 2013). Once the use of ICT is imposed, older people express a general mistrust of the Internet, that then manifests as a mistrust of online internet banking that is imposed (Gurau, 2002; Krebsbach, 2002; Sukkar and Hasan, 2005; Kyriazopoulos, Samanta, Christou, and Ntanos, 2010; Ureel and Wallace, 2013). Older people cited that they had little or no choice in being exposed to what they perceived to be increased risk born out of online financial interactions (Garg, Camp, Lorenzen-Huber, and Connelly, 2011).

As a society, mankind places a great deal of importance on volition (Ryle, 2000). Society treats situations where people are either socially or physically constrained with significance and seriousness. Situations where one's choices have the potential to bring harm and consequence to others bring about the need to control and restrict volition (Frith, 2007; Haggard, 2008). Examples include the need for imprisonment, and the restriction and restraint of a person from entering somewhere, doing something, or saying something through the exercise of a set of laws. Volition is required so that people can make sense of occasions where they are restricted, and come to an understanding of behaviour that is tolerated

and that which is not (Brass and Haggard, 2007). The laws, legislation and rules of society may be seen as necessary components for order and efficiency, whilst the volition and freedom to do what one wants and to say what one believes are the necessary parts to growing our individual humanity (Wegner, 2003). As technology and ICT usage increases, the need to distinguish between volition, choice, and their limits becomes more important (Pew Research Centre, 2014).

Descriptions about the adoption, appropriation, and usage of technology are predominantly made under an assumption that technology acceptance is inevitable (Mendoza et al, 2013; Brown Massey, Montoyo-Weiss and Burkman, 2002). However, the literature on volition and choice makes the distinction between acceptance under freewill conditions and acceptance under forced conditions (Benamati and Serva, 2007). Thus it is important to acknowledge that volition (or the lack of voluntary choice), is a critical area of information for this research because it challenges the idea that usage equates to technology acceptance (Figure 2.2). People make decisions to use technology that are also made under coercion, duress, and a range of external pressures (Brown et al, 2002).
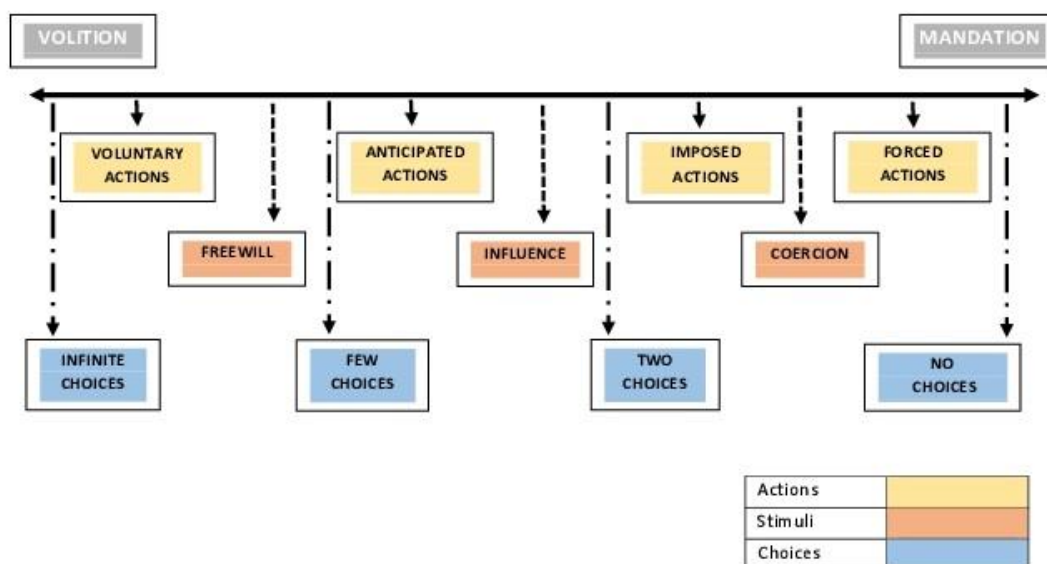
Figure 2.2 Continuum of Volition, Adapted from Haggard (2008)

An environment that supports voluntary use is one in which users identify the decision to use as a deliberate and pressure-free choice (Hartwick and Barki, 1994; Brown, et al, 2002; Mendoza et al,

2013). An environment that uses mandatory technology use is one where users feel compelled to use the technology (Venkatesh and Davis, 2000). Situations that include imposed technology use are closely aligned with mandated technology usage because the choice has been removed to such an extent that there is only a single course of action left and it includes the decision to use a particular technology (Karahanna, Straub, and Chervany, 1999; Mendoza et al, 2013).

2.4.1 Freedom, Social Equality and Fairness

This area of review examines volition and choice as a variable factor that influences trust. Older people exhibit reduced levels of trust where usage of technology is either mandated or imposed (Lawhon, 1996; Benamati and Serva, 2007). Older people foster feelings of doubt and suspicion where imposed and automated banking practices require customers to use online banking to access standard banking products (McKnight, Choudhury, and Kacmar, 2002; Benamati and Serva, 2007). Older people are forced to consider ICT-related concerns about password integrity, privacy, and the protection of personal information (Pavlou, 2003; Rotchanakitumnuai and Speece, 2003; Eriksson, Kerem, and Nilsson, 2005; King, Ureel, Kumar and Wallace, 2013). As a result, they become stressed and anxious (Mendoza, Miller, Pedell, and Sterling, 2013). In many cases the stress has an effect upon the normal decision-making abilities of an older person (Elder, Gardner, and Ruth, 1987; Zeelenberg, Nelissen, Breugelmans, and Pieters, 2008). Decisions on issues connected with money are critical for older people, who in most cases retire under the expectation that they will not need to seek further employment, and can instead live their final years without the need to return to paid employment (Pew Research Centre, 2014). Although some considerations are individual in nature, and include physiological, mental, and educational factors, the mandatory requirement to interact with a technology that can damage an older person's income and stability causes feelings of angst, anxiety, worry and fear (Anderson and Agarwal, 2011).

Once the use of ICT is imposed, older people express a general mistrust of the Internet, that then manifests as a mistrust of online internet banking that is imposed (Gurau, 2002; Krebsbach, 2002; Sukkar and Hasan, 2005; Kyriazopoulos, Samanta, Christou, and Ntanos, 2010; Ureel and Wallace, 2013). Older people cited that they had little or no choice in being exposed to what they perceived to

be increased risk born out of online financial interactions (Garg, Camp, Lorenzen-Huber, and Connelly, 2011).

2.4.2 Mandated and Imposed Adoption and Appropriation

Technology adoption is too strongly associated with a "when" not "if" expectation. The literature associated with the Technology Acceptance Model (TAM), as well as its precursors the Theory of Planned Behaviour (TPB) and the Theory of Reasoned Action (TRA), has overshadowed the problem of acceptance and adoption that comes about from either a mandated or an imposed condition (Mendoza, Miller, Pedell, and Sterling, 2013). The Technology Acceptance Model operates on a normalised premise that technology adoption is inevitable and that the only questions are how and when (Davis, 1989; Venkatesh et al, 2003). Thus much of the TAM proposition carries an expectation that acceptance takes place. In contrast to this volition studies place each new technology or innovation as a 50:50 proposition, that an ICT technology might be accepted or that it might be rejected (Mendosa et al, 2013).

The difference between TAM and Volition is important, because where TAM and other associated technology appropriation models neglect the socio-technical needs of older people (Mendoza et al, 2013), studies that promote volition and choice resonate more strongly with older cohorts (Lindley, Harper and Sellen, 2009; Anderson and Agarwal, 2011, Komiak and Benbasat, 2006). There are two main considerations for the study of ICT volition and choice. The first are ICTs where the usage is mandated. In examples where the adoption of a financial system (for example a bank that only issues its statements online and not in hardcopy form) is a mandate, and where there is no alternative for that system, the absence of choice may see the system used, but not trusted. In such cases the use of terminology such as "acceptance" becomes an inaccurate descriptor for the usage that has taken place.

The second consideration for the study of ICT volition and choice is where although the ICT is not mandatory in the unequivocal sense, there is sufficient expectation and obligation, that usage takes place because of an imposed circumstance (Brown et al, 2002). In instances such as this, it may be that everyone else is using an ICT, and that whilst technically possible to reject the innovation, the anticipation and expectation are sufficiently strong that the imposed usage is perceived as binding and compulsory (Ajzen and Fishbein, 1980). This second consideration for volition is harder to

conceptualise by hard line TAM proponents (Taylor and Todd, 1995, Zuboff, 1988, Brown et al, 2002). Whilst the concept of choice implies acceptance or rejection, those aligned to the technology acceptance methodologies remain expectant that continued usage will bring about acceptance (Venkatesh, Morris, Davis and Davis, 2003). Brown et al (2002) posits: "When individuals *must* perform specific behaviours, the importance of their beliefs and attitudes as antecedents to the performance of those behaviours is likely to be minimized. They might not like performing the mandated behaviour, but they do it anyway, because they are required to do so." Further, the use of technology within a mandated setting exposes the difficulty of the desire to exercise a wilful choice in conditions where the usage is socially, organisationally or procedurally compulsory (Brown et al, 2002; Agarwal and Prasad, 1997, Mendoza et al, 2013)

2.4.3   Reactions and Consequences to Limits on Volition

In conditions where technology use is mandated, the user's freedom of choice is limited. In a work situation, an individual might consider sacrificing their job, however if the assumption is that the individual does not wish to leave the organisation, the choice becomes limited to choices about delaying, obstructing, resenting or sabotaging the new system (Zuboff, 1988, Brown et al, 2002, Mendoza et al, 2013).

Some technologies are diffused at a high organisational level (Rogers, 2003; Henman, 2010). Governments can legislate and sometimes this may remove choice from technology users depending upon the circumstance (Dwyer, 2008; Karger and Stoesz, 2010; Kassim, and Abdulla, 2006). The politics of mandatory practices can be seen both at the nation-state level, and also through to individual firms and corporations (Bhat, 2012). Some states, notably authoritarian regimes where democracy and choice are replaced with compulsory practices, eliminate voluntary technology uptake by reducing the number of choices and competitors (Tan, Corbett and Wong, 1999). Similarly, in a much smaller scale, when a retail business only accepts digital payment through electronic payment systems, then the ability for people to make decisions about almost anything can be aligned with who has the most power, or the greatest strength (Campbell, and Frei, 2010; Arenas-Gaitan, and Peral-Peral, 2015, Mendoza et al, 2013).

2.5   Gerontechnology

Gerontechnology draws together the discipline of gerontology with the context of technology. It covers the influence of technology and innovation on the quality of life for older people (Fisk, Rogers, Charness, Czaja and Sharit, 2009). This literature specifically reveals the need to consider accessibility (Smith, 2008; Caprani, Doyle, O'Grady, Gurrin, O'Connor, Caufield and O'Hare, 2012; Obi, Ishmatova and Iwasaki, 2013), and the cost of technology (Richardson, Weaver, and Zorn, 2005; Cortes, Barrue, Martinez, Urdiales, Campana. Annicchiarico and Caltagirone 2010; Lichtenstein and Williamson, 2006) as characteristics which influence trust and choice (Czaja and Lee, 2007; Pan and Jordan-Marsh, 2010). Although online banking allows for better accessibility in areas of biophysical restrictions (Czaja and Hiltz, 2005; Arenas-Gaitan and Peral-Peral; 2015), there are several references to accessibility limitations. These range from restricted font sizes on online templates and forms (Laukkanen et al, 2007; Wagner, Hassanein, and Head, 2010), to the issue of contrast and visual acuity as a barrier to using technology for banking and financial transactions (Scialfa, Ho, and Laberge, 2004; Conway, 2014).

There are four main areas of consideration in terms of Gerontechnology. The first is the impact of physical, mental and social changes as people age. Older people's lives change with time, and it is important to recognise the value of technology in assisting physical, mental and social changes that restrict the quality of people's daily routines. The second area is concerned with the application of technology changes that incorporate increased accessibility to information and communication with others. The third area considers training and usability. This area draws on new technologies such as virtual reality and augmented reality that enables training scenarios where the person has less restriction from physiological and mental interactions because new technologies enable engagement across a range of virtual and online platforms. Older people are cconcerned that in some cases they have less developed skills and capabilities. The need for increased training that has a focus on usability increases as new technologies place an expectation of greater ICT skill and capability. The fourth area considers the balance between the value of new technologies and the cost of those same technologies. In most instance developers make the assumption that new technologies will benefit users. However in many cases the

benefits of those new technologies needs to be carefully weighed against their cost. Older people often state that there is an increased cost to online banking that includes the purchase of a computer, the cost of a printer, the cost of internet access, and the cost of training. Opinions vary, yet there are significant examples wher older people cite the cost of a new technology as one that is prohibitive in terms of the expected new benefit of its usage.

The analysis and integration of information and knowledge in the area of technology and aging includes issues of age-related decline, access to specific technology, and the use of the Internet (Mayhorn, Rogers, and Fisk, 2004). The digital transfer of communications and the specific areas where technology is gaining acceptance, is the prime direction of gerontechnology (Charness, 2004).

2.5.1 Physical, Mental and Social changes in Aging

Within the discipline of the study of the aging, the examination of social, psychological and biological characteristics is relevant to understanding older people's cognitive learning, adaptation skills, and physical constraints (Lang & Carstensen, 2002). The aging population is negatively associated with ICT usage and adoption (Figure 2.3) and internet usage (Byrne & Staehr, 2006; Chesters et al., 2013; Loges & Jung, 2001; Peacock & Kunemund, 2007; Selwyn, Gorard, Furlong & Lewis, 2003). A wide variety of issues pertaining to aging; overlap with ICT trust, usage, adoption and rejection (Gagliardi, Mazzarini, Papa, Giuli, & Marcellini, 2007; Mollenkopf, 2004).
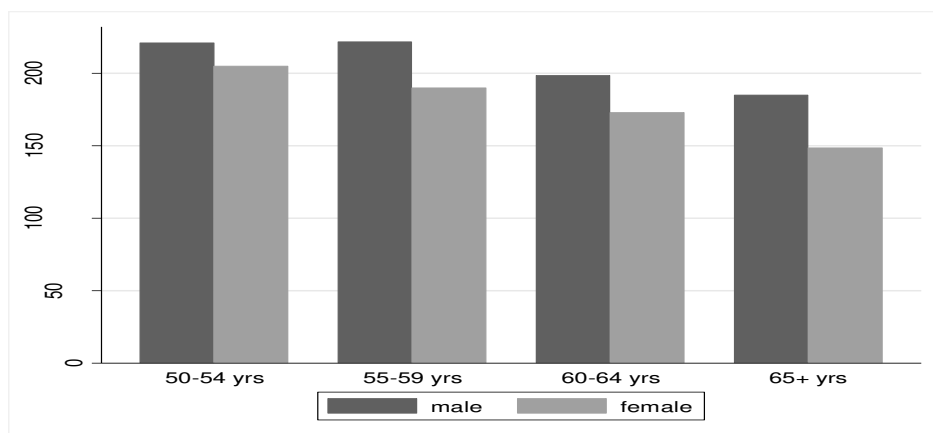
Figure 2.3 Mean Computer Use by Gender and Age in Australia: ABS (2006) in (Chesters et al, 2013)

Aging is a multi-faceted progression where each person is affected by the environment while also influencing aspects of their surrounds (Dannefer, 2003; DiPrete & Eirich, 2005). This progression is accurately described in logical, empirical, and theoretical terms as the cumulative advantage / disadvantage model (Dannefer, 2003, Pew Research Center, 2014). The model describes the aging process as one of great change and adjustment, driven by opportunity and circumstance (Dannefer, 1987; Mirowsky & Ross, 2008). Cumulative Advantage theory (CA) suggests that the rate of adult decline in terms of health is different across levels of education in a manner that progressively enlarges the health gap across most or all of adulthood (McDonald & Mair, 2010). This idea is often quoted as the popular idea that "the rich get richer and the poor get poorer" or the "Matthews effect", but is also applicable to technology acceptance, better education, and ICT trust (Barker, 2012; DiPrete & Eirich, 2005; Merton, 1988; Mirowsky & Ross, 2008).

The effect of increased systems of technology brings a concern about the widening gap between the way in which older people integrate with ICT and how younger generations interact. From a global perspective the United Nations predicts that the differences through levels of education has been widening for decades (UNDP, 2013). Thus whilst the connection between technology and aging is growing with new progress, there are several areas where differences in social, economic, and organizational are establishing problematic dissimilarities. There are numerous information services for users of technology and late or non-adopters in the form of news, information, government services, health, finance, and social support (Pew Research Center, 2014). In this sense the notion that accumulated social capital can influence ICT forms a key part of the discourse on the generational digital divide (DiPrete & Eirich, 2005; McDonald & Mair, 2010; Mirowsky & Ross, 2008; UNDP, 2013). Where socio-economic disadvantage is exaggerated it manifests decreased acceptance of new ideas, changes and skills (Tan, 2011). Older people who use a computer at work are far more likely to have a computer at home (Pew Research Center, 2014). Similarly, older people with higher incomes, and those who are higher educated, are more likely to adopt internet usage and own mobile devices (Pew Research Centre, 2014). The level of activity of each older person is linked to what Activity Theory describes as 'divisions of labour', 'rules', and 'community' (Engestrom, 1987).

In an associated vein, Activity Theory (AT) works on the premise that older people's ability to understand concepts through independent learning, depends heavily upon social interactions (Mechlova & Malcik, 2012). In this context activity theory holds that the range of involvement and engagement in old age tapers when older individuals are compelled to introversion because of social norms, health disabilities, or the death of partners, family or friends (Bai & Guo., 2010; Mollenkopf, 2004). According to Longino and Kart (1982), a distinguishing feature of older people's learning comes through communal interactions. In particular, issues of trusted learning, and higher security issues such as personal information and health information require building a level of trust that only comes in combination with the interactions of, and with, others (Figure 2.4).

The impact of changes from aging are not evenly distributed across the world. In some cases the expectation that technology usage can be widely accessed and used in an environment of ubiquity is important to consider. This is more than simply a question of access. People in remote parts of Australia have differeng requirements in terms of physical, mental and scial change to those in built up and urban areas where technology usage has greater ubiquity and higher levels of development.

In the context of older people who are novice in ICT, activity theory lends strong support to the requirement for face-to-face learning experiences rather than online self-education (Mollenkopf, 2004). The literature explains why many older people are hesitant to engage in a range of activities that might include the adoption of online internet banking. Although best described as a broad, wide-ranging model, Activity Theory includes social contexts, connections to community, and rules and norms define how people interact with objects and outcomes (Mechlova and Malcik, 2012).
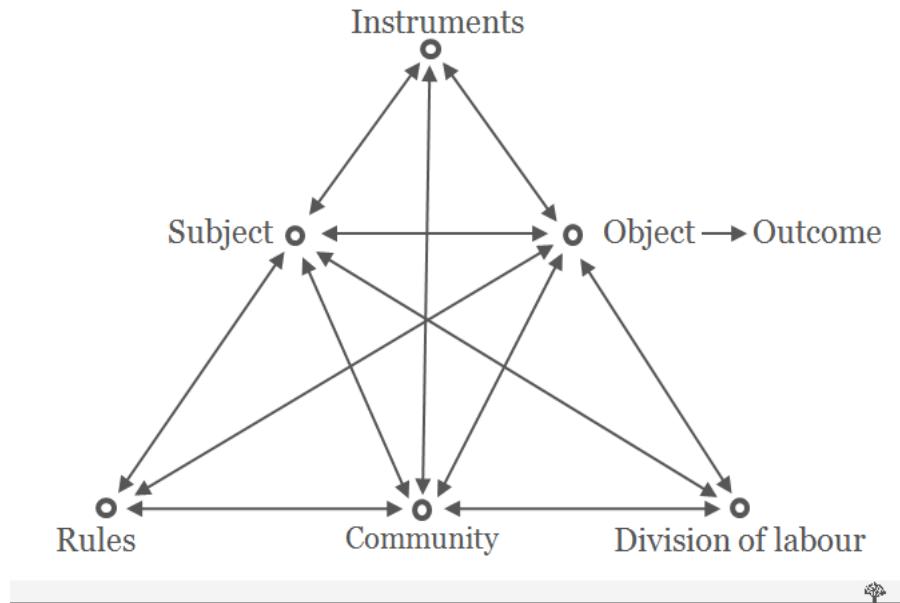
Figure 2.4 A Diagram of Activity Theory (Engestrom, 1987)

A connected theory to Activity Theory is that of Disengagement Theory, first proposed in 1961 by Elaine Cumming and William Earl Henry. The theory hypothesizes that "aging is inevitable, mutual withdrawal or disengagement, resulting in decreased interaction between the aging person and others in the social system" (Cumming and Henry, 1961). Like Activity Theory, this theory bases interaction upon a process of disengagement that is supported by skill deterioration, knowledge limitations, demoralization, and social norms (Harbison, Coughlan, Beaulieu, Karabanow, Vanderplaat, Wilderman and Wrexler, 2012). Disengagement theory is useful in explaining the contradiction that follows internet use (Hogeboom, McDermott, Perrin, Osman, and Bell-Ellison, 2010), where online social networks align with theories of engagement through their networks of reciprocity, and homophily (Heaney and Israel, 2002; Boase, Horrigan, Wellman, and Rainie, 2006) whilst disengagement and rejection of interaction is associated with the isolation and withdrawal that is associated with being active online but physically being isolated from others (Alpass and Neville, 2003; Krantz-Kent, 2005; Harbison et al, 2012). Although there is no direct literature that refers online banking context to these two theories, the general components of both Activity Theory and Disengagement Theory hold parallel thinking to our hypothesis that predicts hesitation towards the perceived risks and lack of trust in mandated and imposed online financial matters.

Socio-emotional Selectivity Theory is a theory of motivation that posits that as people age they become increasingly selective (Jacks and Salam, 2009). This is coupled with older people's preferences for positive information rather than negative information. Thus when trust is sought that relates to a practice such as online banking, any negative information such as security risk will affect the desire to be involved (Bright and Coventry, 2013; Leen and Lang, 2013). Continuity Theory is loosely associated with Socio-emotional Selectivity Theory because it conjectures that even though aging will bring about differences that are inherent to the idea of growing older; many people will attempt to maintain continuity in their activities, their connections and relationships (Berk, 2010). This extends to habitual activities, religious beliefs, and lifestyle choices (Maddox, 1968, Atchley, 1999). As with Activity and Disengagement theory, which have supportive constructs to the hesitation towards ICT systems such as online banking, Socio-emotional theory and Continuity Theory also provide a theoretical explanation for the contested manner in which some older people engage with internet banking whilst others reject it (Berk, 2010).

The psychological change of older people is relevant to the discussion of trusted ICT usage. According to Moschis (1992, p116) "individuals undergo a gradual transformation mentally as well as in the eyes of others and their own". Psychosocial aging affects the way people see themselves amongst their peers. It helps to explain why there are older people who are early adopters of ICT innovations such as online banking. Mattila, Karjaluoto and Pento's (2003) work on Internet banking adoption acknowledges that some mature users of online banking technology were early adopters, whilst most preferred other means of conducting financial banking.

For those born before the middle of the 20th century, it can be anticipated that some older people have less experience with IT as compared to younger generations (Morell et al., 2004). This is attributed to the work/life habits and routines that older people formed before ICT technologies became more widely established. This eventuality implies that older people are at increasingly greater risk to ICT exploitation than in previous years (Morris & Venkatesh, 2000). The rapid transformation to ICT integration has left behind a generation of intelligent citizens who contribute to society in a meaningful manner in all areas of the community except information technology (Rogers et al., 2004). For older people, private transactions such as banking, e-health, along with social media and email

communications, incorporate personal and confidential information within an environment purported to be secure (Tran, 2004). The literature indicates that older people will, with each passing generation, be disadvantaged compared to other age cohorts (Alwadhi and Morris, 2009; Bouma, Fozard, Bouwhuis, and Taipale, 2007). Lack of life experience in the use of technology is likely to translate to technology hesitation and greater risk perception.

2.5.2 Accessibility

There is an informational, educational and cultural divide between older people who are novice at ICTs and the rest of the community (Russell, Campbell, & Hughes, 2008). They are technologically disadvantaged by age (Selwyn, 2004), health (Selwyn, Gorard, Furlong, & Madden, 2003) and financial means (Kim, 2008). Older people are greatly affected by issues of accessibility (Morris & Venkatesh, 2000). The literature repeatedly points to difficulty with accessibility features as important in the acceptance or rejection of new technologies (Hollier, 2013; Plaza, Martin, Martin, and Medrano, 2011). The literature draws inferences towards usage such as banking on mobile devices, where screen size limitations raise the likelihood of marginalising many older people from accessing mobile devices and internet banking (Wu et al, 2009).

Older people experience difficulties with using modern technologies and this can in turn result in difficulties with using innovative technologies resulting in complications with normal societal activity and community interaction and involvement (Mitzner et al., 2010; Virokannas et al., 2000). The ability to read, understand and interpret a range of media as expressed through ICTs under differing conditions such as font size, background screen colour, narration and vocal communication (Fisk et al., 2009; Morris & Venkatesh, 2000; Wilkowska & Ziefle, 2009). Acceptance and roll out to a range of accessibility standards are central to the overall observation from many within the literature (Sheng & Trimi, 2008; Wu et al., 2009) who believe that accessibility features (or more specifically the inability for most web-based instructional security programs to assist with accessibility features) are responsible for an increased number of unsuitable projects (Kobayashi et al., 2011).

In addition to these more established accessibility issues, new emerging trends in smart phones and wearables (Wu et al., 2009), present new technology acceptance issues with size constraints, screen

size and mobile device fragility underscoring challenges for older people (Cortes et al., 2010). Three main accessibility issues are established from the literature. Older people use mobile devices (and specifically smartphones) in a more limited manner than other users because they find the displays hard to read (Kobayashi et al., 2011), the buttons difficult to accurately depress (Gao & Koronios, 2010), and the procedures difficult to master (Kim, 2008; Reneau, 2012). The aging process further aggravates interaction with small screen mobile devices such as smart phones (Wilkowska & Ziefle, 2009). The literature describes a contested acceptance of mobile devices; where new software features compete against the sheer limitations of the devices render new software less effective for the older persons' cohort (Hollier, 2013; Wu et al, 2009).

Accessibility issues have prompted research and development into specialised devices for older people. The '*Raku-Raku*' phone from NTT DoCoMo was one such example of a mobile device with a simplified interface and significantly larger buttons, however devices such as these can perpetuate the digital divide rather than bridge it due to their deliberately different and more limited functionality (Fujitsu, 2012; Kobayashi et al., 2011). The Raku-Raku is one of a new generation of mobile devices that use haptics to extend the sense of physical and analogue interaction by older people (Priplata, Niemi, Harry, Lipsitz, and Collins, 2003; Fujitsu, 2012). The literature indicates that whilst there are various software innovations that assist greatly with accessibility, these improvements are not consistently deployed within the market, and many new concepts have yet to be accepted, trusted, or consistently relied upon.

2.5.3   Training and Usability

Access and availability to training, education, and skills development are influential in measuring perceived ease of use (Chesters et al., 2013; Kim, 2008). Access to training and skills development identified benefits for older people in terms of higher self-efficacy and lower computer anxiety (Karavidas, & Katsikas, 2005). Feelings of competence, enhanced self-esteem, and short term memory have all been attributed to increased levels of training and computer usage (Cortes et al., 2010; Lam & Lee, 2005; Lawhon, Ennis, & Lawhon, 1996). Even after receiving training and induction in commonplace ICT activities such as correspondence using email, research indicates that many older

people have difficulty being able to perform tasks (Cook et al., 2011a; Gatto & Tak, 2008). The literature strongly portrays a culture of poor usability that restrains and restricts older people from greater access of ICT innovations (UNDP, 2013).

In this sense, training and usability models that can inform the better engagement with technology for older people are an essential part of understanding trusted acceptance. Many new innovations focus on the ease of access in using new technologies, when for older people the emphasis is more critically focused on the need to train older cohorts so that they have the skill and capability to use new technologies more readily. It is difficult to envisage that older people will readily look to use new ICT technology if they perceive that their usage of the technology will be less fluent, less confident, and more inaccurate than other users. The literature poinst to a need for greater emphasis on the upskilling of older people in order to facilitate greater perceived acceptance of technology usage.

Adaptation skills are specifically linked with the main focus of gerontechnology: aging and technology (Hill, Beynon-Davies, and Williams, 2008). The usability of new ICT innovations, together with the method of training, especially whether the training can be undertaken in a form that does not require using the Internet, are key differentiators between the behaviour and trust of ICTs by older people and their younger counterparts (Yap, Wong, Loh and Bak, 2010; Lee, Kwon, and Schumann, 2005).

2.5.4   Cost of Using Technology

The cost of technology impacts on the decision-making of older people to determine how engaged with ICTs they become (Kim, 2008; Russell et al., 2008: Selwyn, Gorard, Furlong, & Madden, 2003). For those older people with sufficient financial means the adaptation to a nation of National Broadband Hi-Speed connectivity provides another step in the way society changes its method of communicating (NBN, 2012). However, studies on people from lower socio-economic situations reveal an under-reported impediment in the financial capabilities of aging retirees to cope with the cost of updated routers, computing equipment (Cortes et al., 2003), ongoing broadband access fees (Stankovic, Insup, Mok, & Rajkumar, 2005), and the cost of learning and up-skilling in line with their daily needs (Morris, 1994; Phang et al., 2006). A study of online banking adoption in Finland (Mattila et al., 2003)

discovered that household income was a significant barrier to the adoption of Internet banking by mature customers.

This indicates there is a proportion of the older persons' community who are finding the cost of internet access to be beyond their limits, and that there is an accompanying issue in terms of computer literacy and familiarity that makes some daily tasks not only cost prohibitive but also socially alarming (Eastman & Iyer, 2004; Reisenwitz, Iyer, Kuhlmeier, & Eastman, 2007; Saunders, 2004). In a global sense, the literature points to a world that is far from accessible by the older cohort. In developed countries the use of technology enjoys greater usage by older people, however even within this grouping there is resistance towards online banking technology and innovation (UNDP, 2013). There is a strong theme of cost prohibitive opposition from older people towards technology (Morrell, Mayhorn, and Echt, 2004; Macedo, Petronilho, and Caine, 2013; Cook, Randhawa, Large, Guppy, Chater, and Ali, 2014).

Recent changes to the Australian Government Centrelink policy on welfare and pension statements reveals that customers (including all older citizens) no longer receive statements via post after July 1st 2012, but instead will be able to download information via the Internet or through the Department of Human Services Centres (DHS, 2012). Official policy changes such as the Federal Government digital statement program means that older people are further marginalized towards a forced acceptance of ICT for their daily informational requirements (Australian Government, 2013). For older people who are novices at ICTs this means an increased reliance on third parties, relatives, or friends (Fealy, Donnelly, Bergin, Treacy, and Phelan, 2012). Additionally, in many cases paid carers/agents, (Fast, Keeting, Derksen, & Otfinowski, 2004) therefore increase the cost to pensioners for information that they would previously receive by mail (Cortes et al., 2003; Ott, 2000). This indicates an increasing trend towards imposed and mandated systems in the areas of banking, social security and health (Reinders, Dabholkar, and Framback, 2008; Schmidt, 2015).

There is also an additional risk through the use of third party assistants and carers who are put in positions of implied trust, with access to older people's life savings, and control of a range of income and outgoing expenditures (ANPEA, 2008; Manthorpe, Samsi, Rapaport, 2012). Issues pertaining to autonomy remain at the forefront of widespread trust concerns (Ott, 2000). Whilst there are multiple

examples of embedded e-Tools specifically designed for assisting with agent technology, the ongoing issue for novice older people remains with the fundamental problem of older people's trust in ICT (Cortes et al., 2003). Older people remain wary of ceding their physical financial control to both a third party agent, and essentially a third party infrastructure. For those in aged care, the physical restriction that necessitates reliance upon others for online banking also drives their uncertainty towards trusting technologies that remain beyond their grasp (OFT, 2012).

A similar problem to pension and welfare access exists with banking. Whilst the big four Australian banks (CBA, Westpac, National and ANZ) have a similar existing policy to Centrelink that encourages but does not force the use of e-statements (ASIC, 2013), those banks with international origins (Citibank, Chase, JP Morgan) have shifted to e-statements only. Statements are not available through the post, and reconciliations are not available in face to face meetings or over the counter exchanges for these banks (Citibank, 2013; HSBC, 2013). In a move that now eliminates the posted paper statement (or charges for one), the policy direction is clearly shifting towards e-statements (Print21, 2013). The literature demonstrates the increasing deployment of imposed and partially-mandated ICT systems in the areas of finance, health, and online banking.

The combination of trust and knowledge in ICT can present a difficult challenge for novice older ICT users (Australian Government, 2013). Financial deregulation of the banking markets has been deemed as a successful policy that has brought about better competition, a wider range of banking products, and the liberalization of market capital (APSC, 2012). As a strategy, deregulation is acknowledged as purposeful. In practice, however, a deregulated financial market has also seen considerable trimming of the community-based banking policies that once went hand in hand with face to face banking. Of the more affected areas, older people now endure considerable hardship from on-line statements, account access and transfer procedures, and increased risks from identity predators and manipulators. The policy of the future regarding statements is trending towards an exclusively e-centred domain (APSC, 2012). In order to access one's account the consumer will have no alternative than to use the Internet (Bitterman & Shalev, 2004; Charness & Root, 2009).

2.6 Trust, Governance, Authority, and Risk

This section discusses trust, then discusses governance, and then connects the two areas by discussing the way in which they connect with authority and influence. The section then discusses risk, and compares potential threats within the context of trust, governance, and the system of controls that influence and regulate their impact (Figure 2.5).
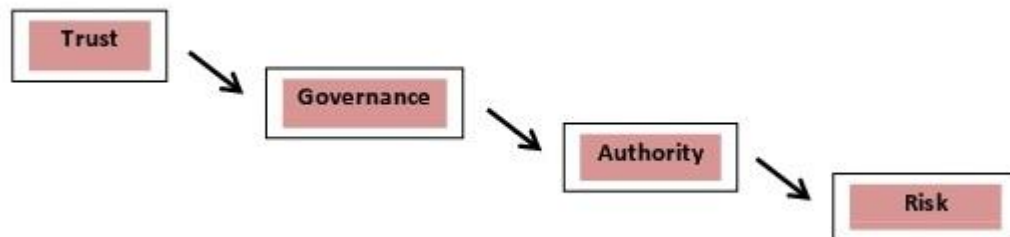
Figure 2.5 Diagram of ordered review of literature relating to Trust, Governance, Authority, and Risk.

This literature establishes the presence and absence of trust assumptions upon which mandated ICT practices can be evaluated (Govindan and Mohaptra, 2011; de Souza, da Silva, da Silva, Roazzi, and da Silva Carrilho, 2012; Lawlor, 2014). The literature points to a gap between the compliance and regulatory language which underpins the use of technology for financial banking (Grabner-Krauter and Faullant, 2008; Fealy, Donnelly, Bergin, Treacy, and Phelan, 2012) and the more human, peer driven trust that develops between older citizens (Moutinho and Smith, 2000; Grundy, 2005; Metlife Mature Market Institute 2009; Lin 2011). Mandated and imposed financial systems emphasise the security, safety, and reliability of specific applications and programs (Advocacy and Rights Centre, 2008; Grabner-Krauter and Faullant, 2008) whilst older people interpret new systems as impositions over already functioning banking methods with disdain, doubt and suspicion (ANPEA 2008; Lin, 2011; Arenas-Gaitan and Peral-Peral, 2015). One prominent theme in the literature centres on elder financial abuse, where imposed ICT banking for older people and frail people leads to banking and asset exploitation by family and known associates and acquaintances (Setterlund, Tilse, Wilson, McCawley and Rosenman, 2007; Kurrle and Naughtin, 2008; Manthorpe, Samsi, and Rapaport, 2012). The literature suggests instances of financial abuse that occur as a result of online banking access by others,

and the difficulty experienced by older people who prefer to conduct their financial business via face to face physical means rather than through the Internet (Lachs and Pillemer, 2004; Abbey, 2009; Davies, Gilhooly, Gilhooly, Harries, and Cairns, 2013).

2.6.1 Trust

The 2014 report on *Older Adults and Technology Use* refers to the majority of American older people living in isolation from ICT technology (Pew Research Center, 2014). Older people stipulate apprehension about engaging with technology as a result of two trust-related barriers (Neogi and Cordell, 2010).

2.6.1.1 Individual Limits to Capability, Understanding and Education

The first barrier is a hesitation to use ICT and to limit technology use because of a perceived lack of understanding, training, and technical ability (Karavidas, Lim, and Katsikas, 2005; Chu, Huber, Mastel-Smith, and Cesario, 2008; Masi, Suarez-Balcazar, Cassey, Zinney, and Piotrowski, 2003). By citing a lack of trust in themselves, and those involved in training, older people highlight the need to assist those amongst their cohort who are generationally predisposed towards daily routines that are not ICT dependent (Rice, 2002; Caplan, 2007). Of these routines - banking, finance, and bill paying are repeatedly cited in the literature as elements that require trusted capabilities (McCloskey, 2006; Eastman and Iyer, 2004). These capabilities also relate to governance, since ICT – driven systems need to follow a regulatory structure that ensures that people with low levels of ICT literacy can proceed with a realistic expectation of a trusted experience (Neogi and Cordell, 2010).

There is a contested understanding about the different areas of governance, asking whether the governance issues facing older people in banking are issues of internet governance or of financing and banking regulations (Lessig, 2000; Neogi and Cordell, 2010). The literature also points to the need for choice rather than mandatory practices, with older people seeking pathways that give alternatives to imposed and enforced ICT systems for daily activities such as banking (Lepa and Tatnall, 2006). There are high levels of anxiety amongst older people with neophyte understanding of ICT (Karavidas, Lim, and Katsikas, 2005). This ranges from mild angst, apprehension, and group think, through to high level

technophobia and computer-related anxiety (Australian Government, 2013; Mikkola, and Halonen, 2011).

2.6.1.2 Trust in Technology, Reliability, and Systems

The second trust barrier is focussed on the confidence and expectation that ICT systems will operate reliably and to the satisfaction of the user. The literature points to failure to trust relationships with online systems where human contact is limited, and where the reliance falls to a faith and conviction in the reliability of the technology (Mollenkopf and Fozard, 2004). Older people indicate widespread misgivings about systems where the human component is less visible, and where questions and inquiries are directed to nameless, faceless points of contact (Cohen, 2001; Mollenkopf, 2004). Other worries focus on the perceived likelihood and consequence of security problems, in particular identity theft, financial theft, privacy breaches, and data loss (Australian Government, 2013). There are signs that older people have little trust in cloud systems, or in data storage outside of Australia (Noor and Sheng, 2011). Older people hold perceptions based on cultural values that centre on the trust associated with the tangible rather than the virtual, and the human rather than the automated aspects of information technology (Kvasny, 2006).

Novice ICT users are subject to widespread vulnerabilities (Cohen, 2001; Hogeboom, McDermott, Perrin, Osman, and Bell-Ellison, 2010). Some of these vulnerabilities are in the area of trust and usage, and apply to users in general; however the majority of the vulnerabilities are specifically problematic for novice users (Australian Government 2013; Carlson, 2006). The connection to social behaviour rather than technical ability (Vergeer and Pelzer, 2009, highlights the distinction between mandated and voluntary interactions is an important factor in ascertaining differences about how older people trust and use ICTs (Chan, Thong, Venkatesh, Hu, and Tam, 2010).

A major gap in the literature is that far more has been written about the acceptance of innovations than the rejection of them (Rogers, 2003). There is an implied assumption that innovation will either be accepted straight away or eventually, however very little explains those users of innovation who repudiate, or wish to reject, the acceptance of ICT (Mollenkopf, 2004). There are two

contests in terms of mandated and imposed technology. The first is where older people are directed to adopt an ICT-based change from an existing non-ICT practice. People asked to shift from face to face banking to the practice of online internet banking fall into this category (Pikkarainen, Pikkarainen, Karjaluoto and Pahnila, 2004). The second relates to currency where older people are expected to shift from one ICT to a different ICT technology (Morrell, Mayhorn, and Echt, 2004). People asked to shift from one browser such as Internet Explorer to Mozilla Firefox for the purpose of internet banking and browser-security fall into this category (Ye, Seo, Desouza, Papagari, and Jha, 2006; Dormann and Rafail, 2006). Older people are confused about secure web browsers and the usage of one IT device over another (Lin, Chan, and Wei, 2006; Chen and Hitt, 2002; Ranganathan, Seo, and Babad, 2006). Novice users and late adopters of technology associate mistrust with technology that is mandatory. There is an inverse correlation between trust, and mandatory usage, of ICTs (Lee, 2009; Mollenkopf, 2004). Similarly, people forced to leave one ICT for another under mandatory conditions associate less trust with the mandated ICT (Morrell et al, 2004).

2.6.1.3   Trustworthiness, Usage, and Acceptance

Technology acceptance and usage underpins much of the focus in understanding trust. There is an expectation that it is difficult for an innovation to be accepted into society without the ability for its consumers to use it (Grimes et al., 2010). Thus the evolution from diffusion through technology acceptance represents an historical depiction of multiple iterations of acceptance models – each one attempting to get closer to issues of trust and reliance (Rogers, 2003; Venkatesh and Bala, 2008). Technology acceptance models make a strong connection between usages and trust (Venkatesh, Morris, Davis, and Davis, 2003). This is not helpful where that usage stems from a mandated or imposed circumstance. However, there are models outside of the previously discussed TAM / diffusion / norms / beliefs / behavioural intention suite of considerations that look at how new innovations (Kvasny, 2006). The Technology Readiness Model describes a closer connection with trust (Diako, Lubbe, & Klopper, 2012), taking into consideration variables such as discomfort and insecurity (Brush, Edelman and Monolova, 2011; Westjohn, and Arnold, 2007; Chen and Li, 2010).

Examples of challenges to trust in technology can be seen in the form of domestic identity theft (Sylvester, 2004: Mordini, Wright, Wadhwa, De Hert, Mantovani, Thestrup, Steendam, D'Amico, and Vater, 2009). This proliferates amongst older people where elder financial abuse is practised by family members and close acquaintances for the purpose of material gain (Rengamani, Upadhyaya, and Rao, 2010). In situations where older people do not trust their own abilities due to limited ICT skills and confidence, they are forced to trust others even in situations where they fear trust is being abused (Rengamani, Upadhyaya, and Rao, 2010; Eggermont, Vandebosch, and Steyaert, 2006; WSAB, 2015). There is a need for greater regulation and authority in terms of older people, their carers, or their family members, and their access to financial accounts and assets (Dyer, Heisler, Hill, and Kim, 2005; Wagner, Hassanein and Head, 2010). Further, older people understand the potential risk of online financial elder abuse and in some cases resist ICT as a protective measure (Clare, Blundell, and Clare, 2011; ABS, 2012; Soar and Yu, 2014)

Older people identify strongly with the concept of trustworthiness (Wagner, Hassanein and Head, 2010). Although it takes the conformity of a single person to accept an ICT system, trust is more correctly defined as a "property of relations between two or more social actors" (Morwczynski & Miscione, 2008, p288). Social actors in this context can vary from individuals to corporations, associations or businesses (Kuriyan, Kitner, & Watkins, 2010). For some older people the idea of trust relies very strongly upon the need for *trust* to be associated with a trusted relationship. The need therefore extends to another person (or group) with whom a set of expectations and beliefs can be established (Wagner et al, 2010). Older people cite that the absence of a second party equates to the absence of trust (Tanis and Postmes, 2005). Some older people will trust an ICT based upon a connection with a second person or persons, but not based upon a relationship with a human-less piece of technology (Grimsley and Meehan, 2007; Vimarlund and Olve, 2005).

2.6.1.4   Measuring Trust

Trust is strongly associated to risk. It can further be defined as:

> "... the willingness of a party to be vulnerable to the actions of another party based on
> the expectation that the other will perform a particular action important to the trustor,

irrespective of the ability to monitor or control that other." (Mayer, Davis, & Schoorman, 1995, p710)

Measuring trust can be problematic, however the Technology Readiness model (TR) is used to measure citizen partiality to embracing new innovations in work and outside-of-work situations (Parasuraman & Grewal, 2000). It is designed to consider trust alongside acceptance (Diako et al., 2012) and is an attitudinal construct (Westjohn, Arnold, Magnusson, Zdravkovic, & Zhou, 2009). The TR model examines the inclination of an individual to use technology by four character traits that include optimism, innovativeness, discomfort and insecurity (Chen & Li, 2010). These qualities (see Figure 2.6) are considered as key determinants in assessing someone's frame of mind towards embrace innovative technology (Lee, 2009; Walczuch, Lemmink, & Streukens, 2007). This model is helpful in classifying later adopters, but does not adequately explain the differences that arise from imposed and partially mandated technology upon older people (Diako et al., 2012).

The Technology Readiness Index (TRI) classifies against five categories of innovation recognition including: innovators, early adopters, early majority, late majority, and late adopters (Parasuraman, 2000; Parasuraman & Grewal, 2000; Walczuch et al., 2007). It is often depicted in connection with the Technology Acceptance criteria of PU and PEOU (Walczuch et al., 2007). The TR index presents a model that is more clearly able to consider both the influencing determinants of trust (optimism and innovativeness) and also the determinants of mistrust (insecurity and discomfort) (Walczuch et al., 2007). These factors of influence are present in online banking scenarios (Charness & Boot, 2009) and also at automatic teller machines where older people are required to interact with technology rather than in a face to face exchange (Fisk et al., 2009).
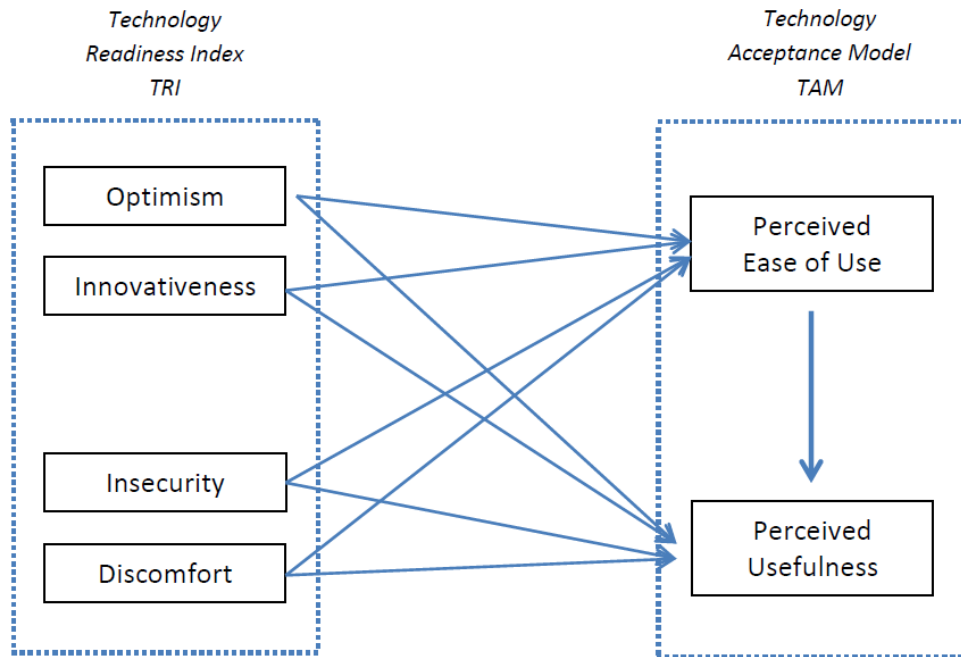
Technology Readiness Index (TRI) alignment with TAM adapted from Walczuch et al. (2007)

Figure 2.6 The Technology Readiness Index (TRI) alignment with TAM. Walczuch et al. (2007)

Whilst predominantly described as a social construct, trust in ICT is also described as trust in a system. Trust can be described as a collection of components which another component can rely on. Where component A trusts component B, that trust is broken if B violates the properties that enable the approved functionality of A. Here trust depends on the accurate and appropriate interaction of two or more components within a predetermined set of limits (Verissimo, Correia, Neves, and Sousa, 2008). In ICT terms the limits of components trying to interact appropriately is termed the trustworthiness of each trusted component. The trust that might be placed in an internet banking system is therefore best expressed as a set of components interacting within the limits of each component's trustworthiness in completing some form of interaction with another component (Kelton, Fleischmann, and Wallace, 2008).

2.6.2 Governance

Rhodes (1996) in his seminal work on governance offers six definitions of governance. These definitions are all aimed towards achieving a universally applicable system of authority. He describes changes where globally technological advancement is accompanied by influence and authority from individuals to corporations and by public to private interests. The last two of his definitions (socio-cybernetic systems and self-organizing networks) support a system of order where ubiquitous ICT is partnered by discussions, understandings and rules that pass freely between stakeholders, hierarchies, and embedded systems of authority. In this sense e-governance does not readily accept mandatory ICT systems, but rather looks to broaden system authority to include choices ranging from inclusion to rejection. E-governance embraces participatory management and influence (Sassen, 2003a; Tait, 2014). Yet at the same time it draws considerable legitimacy from its openness, accountability, reciprocity and pluralism (Perri, 2005; Bevir, 2009).

E-Governance takes on greater importance as cyber security, cyber operability, and cyber compliance form a substrate through which internet and computer-technology rises and falls against a changing backdrop of trust (Gatto and Tak, 2008). The decision making process for older people goes beyond a simple choice about acceptance of an innovation (Carlson, 2006, Hogeboom et al, 2010; Blanton, 2012). The integration of deciding about trust and mistrust is influenced by a range of factors extending to reliability, assurance, privacy, capability, openness and governance (Gefen, Karahanna, & Straub, 2003; Niehaves & Plattfaut, 2010). The relationship between online parties such as banks and businesses, and their customers makes it clear that an e-vendor is more than its ICT connection (Grimes, Hough, Mazur, and Signorella, 2010). Older people expect that arrangements involving online ICTs will incorporate a range of human qualities centred on trust (Chang, McAllister, and Caslin, 2015).

These include the notion that any transactions are thoroughly dependable, credible, and without risk (Gefen, et al., 2003). Thus when the realities of online security risks, attacks and the targeting of older people's assets are superimposed over any given innovation, the decision to trust an ICT innovation becomes a more complex matter than acceptance of the technology based on its ubiquity (Diako et al., 2012; McKnight et al., 2002; Suh & Han, 2002).

The rules, regulations, and conventions that shape and control the way in which older people interact with ICT are intended to guide the manner in which older people accept or reject innovation and change (Mujtava and Pandey, 2012). Innovations that are more strongly connected with activities that have some element of imposed requirement are useful in determining the way in which trust impacts on innovation acceptance (Ott, 2000). Banking is one such activity that has an imposed quotient that is instructive in discussions about trust and ICT acceptance (McKnight et al., 2002). Online banking provides a stronger connection to mandated actions than general ICT usage on the Internet that might involve email and social media interaction Benamati & Serva, 2007). Banking and asset protection is of extremely high importance to older citizens (Ott, 2000). The transition from face to face banking services to online interactions using ICTs requires critical decision making (for older people) and imposes acceptance of technology usage in order to access a range of financial exchanges (Benamati & Serva, 2007; Lee, 2009). The literature demonstrates that older people perceive vast differences in the regulatory operations of face to face banking and that of online banking interactions (Neogi and Cordell, 2010; Chan et al, 2010)

Governance-framed perspectives of the differences between virtual/online and face to face/real-world manifestations reveal difficulties in accepting ICT innovations that incorporate trust (Charness & Boot, 2009; Grimes et al., 2010; Ott, 2000). For older people the shift from physical and face to face security to online security is sharp in contrast (Mattila, Karjaluoto, and Pento, 2003). It includes issues of trust, shifts in physical and virtual requirements, and in many cases additional costs in technology (Phang et al., 2006). There are clear distinctions between online governance and real world governance (Peacock & Kunemund, 2007).

Governance takes on a different form in its ICT version (Chan et al, 2010). Here the emphasis is upon new modes of governance, such as informal participation, social media commentary, and community-based groups and assemblies (Sassen, 2003a; Rhodes, 1996; Walters, 2004). Governance refers to processes and practices that enable individuals, groups and organisations to apply power, authority and influence (Bannister and Connolly, 2012). Governance is more powerful than

government and government is described as a subset of governance (Walters, 2004). Governance is a multilevel authority that incorporates the complexities of operating on multiple levels. Governance has the capability of self-regulation, as well as operability across boundaries and across networks (Bevir, 2009). It is multi-scalar and applies both vertically and horizontally through hierarchies, frameworks and processes. The method of action and change of governance is best described as "steering" and not "rowing" (Rhodes, 1996). It is this type of governance that translates into e-governance,

The e-Governance of mandatory and imposed technologies follows these new participatory modes of governance (Walters, 2004; Latham and Sassen, 2005; Perri, 2005; Tait, 2014). It recognises a much broader range of stakeholders and influencers (Sassen, 2003a). Whilst there are several contested definitions of e-Governance, those pertaining to trust in mandated and imposed ICT systems are clearly focused on new modes of governance. E-Governance can be described as a much more all-encompassing form of authority than e-Government (Tait, 2014). As a multi-scalar concept, e-governance is more suited to interacting with all forms of digital technologies. Electronic markets, internet knowledge archives, social networking, SMS messaging and a range of utility logic systems can all represent interconnecting actors from both private and public spheres (Latham and Sassen, 2005; Paetau, 2003).

There is an expectation on the part of older people that online financial experiences must be risk free and free from duress and complexity. The literature suggests that such expectations are unrealistic, and that financial providers operate under the working assumption that late adopters will in the end coalesce (Pew Research Center, 2014)

2.6.2.1 Models of Trust

There are many models, frameworks and examples of an underlying assumption that it was not if, but when, an innovation would gain acceptance (Venkatesh and Davis, 2000; Pavlou, 2003; Keat and Mohan, 2004; Gefen, Karahanna and Straub, 2003). However other research describes the more multidimensional connections that older people grapple with in terms of their trust and/ or mistrust of ICT innovations (Lewicki, McAllister, & Bies, 1998). In these models the notion that an innovation has multiple facets to its consideration allows for the more complicated understanding that an

innovation can be trusted in one sense and yet not in another (Chang, McAllister, and McCaslin, 2015) (Table 2.1). Even considerations relating to free applications for online banking carry a heavy weight in terms of trust and governance. An example might be how an older citizen reacts to an expectation to adopt an online banking solution in the form of a free online app when a previously free bank statement now has a cost (Davis et al., 1989). Table 2.1 illustrates the distinction between "No Trust" and "Distrust". Where the "No Trust" column is characterised by a lack of trust, confidence and faith, the column "Distrust", describes much more deliberative approaches that show an intention to question a technology with a sense of purpose. Both column elements may lead to technology rejection, however the "Distrust" column appears far more purposeful, resolute and persistent in its approach.

Table 2.1 Integrating Trust and Distrust in Online Banking

	No Distrust	Distrust
No Trust **Characterised by:** **No hope** **No faith** **No confidence** **Passivity** **Hesitance**	Ambivalence **Casual acquaintances** **Limited interdependence** **Arms-length transactions** **Professional courtesy**	Blind Suspicion **Undesirable eventualities (expected or feared)** **Harmful motives assumed** **Interdependence carefully managed** **Preemption: Paranoia** **Interaction occurs only as required** **Monitoring of behaviour** **Attending to potential vulnerabilities**
Trust **Characterised by:** **Hope** **Faith** **Confidence** **Assurance** **Initiative**	Blind Trust **High value congruence** **Interdependence promoted** **Opportunities pursued** **New Initiatives**	Bounded Trust **Trust but verify** **Relationship Highly segmented and bounded** **Relationship limited to aspects of relation** **(where trust is engendered)** **Relationship Restricted (Where distrust is present)** **Opportunities pursued but downside risks are closely monitored**

Integrating Trust and Distrust in online banking. (Lewicki et al. 1998)

Trust is closely linked with acceptance and usage (Venkatesh and Bala, 2008; Rogers 2003; David, 1986), and yet there is a repeatedly reinforced notion that trust is more complex than a simple relationship (Bagozzi, 2007; Benamati, 2007; Turner, Kitchenham, Brereton, Charters, and Budgen, 2010; Ferreira, Torres, Mealha, and Veloso, 2015). No single usage is enough to confirm trust, although it may contribute towards the growth of a trusted perception. Trust does not occur and remain in a static sense. Trust builds "over time" (Ott, 2000). Trust can move forward or backwards based upon the interactions between solutions and problems (ANPEA, 2008; Australian Government, 2013; Carlson, 2006). As different problems and results are communicated back and forth, trust changes (Lee, Kwon,

and Schumann, 2005). Trust occurs and changes through the sharing of knowledge and the socialisation of ideas (Rogers, 2003). Trust depends upon social groups expressing their thoughts through the shared communications of communities (Dekimpe, Parker, and Sarvary, 2000).

The Social Construction of Technology (SCOT) approach (see Figure 2.7), describes the variables of trust building with technology (Hossain & Wigand, 2006). The SCOT framework regards trust as a complex process created "over time". Such a progression requires multiple experiences and discussions in order to create a set of social interactions that share knowledge of what to trust, and in what form the trust might exist (Tatnall and Lepa, 2003). When viewed as a set of intellectual and knowledge assets, trusted elements begin to grow as more users collaborated and exchange their views and experiences. Higher levels of trust in ICTs require trust amongst parties. It is a set of complex perspectives and communicated ideas, derived by experience, discussion, thought and usage. It requires integration with tangible and physical assets as guided by shared collaboration (Hossain & Wigand, 2006). This Social Construction of Technology approach relies heavily on the socialisation of ideas. The SCOT method aims to derive solutions to ICT problems based upon a multifaceted exchange of ideas between different social groups (for example older people). It offers alternative explanations to the more widely published technology acceptance literature (notably TAM) and allows for differentiation in how people are classed as possible non-adopters rather than simply late adopters (Lee, Kwon, and Schumann, 2005).
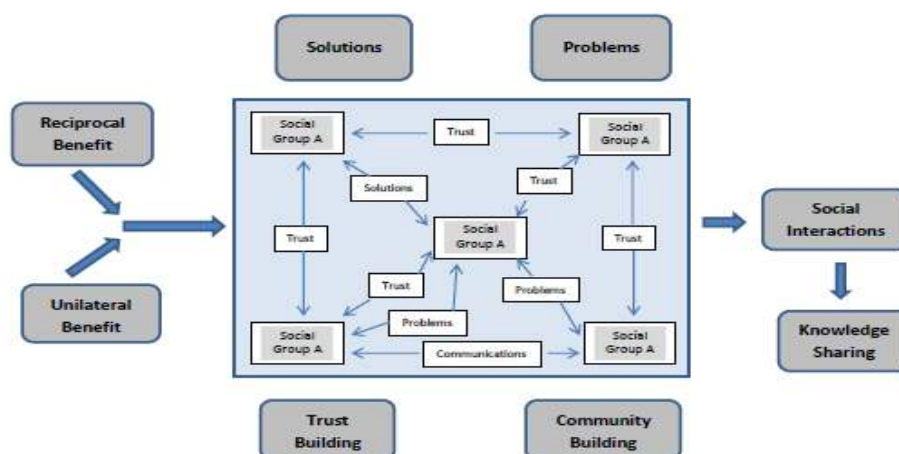
Figure 2.7. The Social Construction of Technology (SCOT) approach (Hossain and Wigand 2006)

In drawing on the importance of social exchange of ideas, the commitment-trust theory can be used to understand in greater detail the importance of relationship building (Rotter, 1967; Morgan and Hunt, 1994; and Kassim and Abdullha, 2006). The theory suggests that trust is not just about forming a level of trust about a product or innovation, but also requires the forming, and continued use, of a relationship between the parties (see Figure 2.8). The theory places a greater level of importance on what it terms as 'key mediating variables' (KMV) in stating that the relationship between the vendor and the client is more important than the trust level held with the product (Morgan and Hunt, 1994). Whilst the model does not work well in scenarios of mandatory or imposed use, this is offset by the emphasis upon the relationship between the vendor and the client. Commitment-trust theory is dependent upon the relationship between parties (not the product) continually developing "over time" (Kassim and Abdullha, 2006).
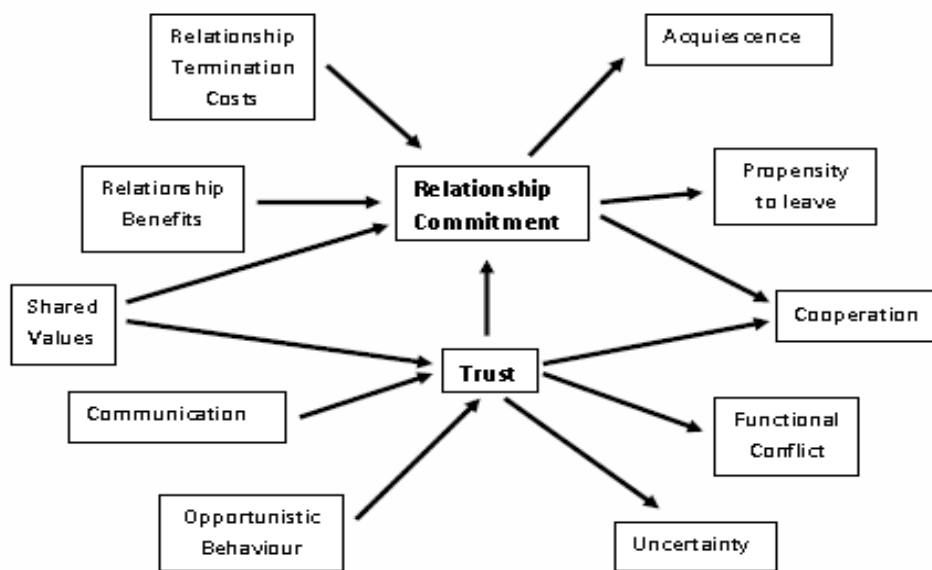
Figure 2.8. The Key Mediating Variables in the Commitment-Trust theory
Adapted from Morgan and Hunt (1994).

2.6.3   Trust, Authority, and Influence affecting Governance

The crossover between trust and governance can be described as the distinction between hard and soft governance. This crossover is an important consideration in understanding the digital divide between older people and others (Mordini et al., 2009). It suggests that cultural issues dominate over concepts of hard governance (Alston, 2014). Soft power in the form of community-based exchange of

ideas is more accepted by older citizens because of its much greater participatory structure (Suh and Han, 2002). There are multiple studies that show the desire for older people to be involved in technology and innovation (Kuriyan, Kitner, & Watkins, 2010; Pikkarainen, Pikkarainen, Karjalouto, and Pahnila, 2004). However, there is a corresponding reluctance to accept financially-related imposed and enforced scenarios whilst simultaneously learning to use them (Saunders, 2004). In cases where older people are being asked to trust and use a technology whilst understanding and adjusting to a new form of ICT, hesitation, delay, and resistance become barriers to the usage (Wilkowska and Ziefle, 2009). In some cases, it might simply be a shift to the use of an online technology rather than a face to face interaction and exchange (Saunders, 2004; Wilkowska and Ziefle, 2009).

Alston, (2014) highlights the setting where older people are attempting to adjudge trust in ICTs by attempting to understand the culture of its rules and its structure. Older people take a soft approach to governance that evaluates the culture of the innovative practice (for example online banking) using values and principles that they already hold. At the same time older people have an understanding of the need for the hard governance of ICT, where a structure of compliance, technical reliability and standardisation forms the regulatory structure that banking organisations incorporate into online banking (Sassen, 2003a; Vincent and Harris, 2009; Bevir, 2009). There seems to be a requirement for a hybrid of both soft and hard elements in ICT-based governance (Raab, 2006).

This area posits the need for high-level compliance and data protection alongside the incorporation of participation and engagement with individuals and citizens' groups with a greater level of social inclusion (Burmeister, 2010; Goujon and Flick, 2010). Going further, there is a great deal of momentum on the need to grow the right culture of trust for change to occur (Alston, 2014). Organisations and their ICT products need to exhibit consistently believable levels of trust (Salter, 1999), because there are several perils that create an environment for mistrust to take root (Alston, 2014). This push for change suggests a mis-match between the culture of enforced compliance of ICT governance and the expectation of participatory governance on the part of older people people considering technology adoption.

2.6.4 Risk

Risk is typically defined in terms of uncertainty (Figure 2.9). It is described as the trustee's belief or about the probability of advances and/or damages (Mayers et al., 1995, p710). When risk is present, trust becomes mandatory (Belanger & Carter, 2008; Pavlou, 2003). Similarly, when trust is present, perceived risk decreases (Pavlou, 2003). Risk is problematic to quantify tangibly, and the literature often therefore reverts to a preferred description of perceived trust (Campbell, Carter, Hobbs, & Schaupp, 2012; Kuriyan et al., 2010; Reisenwitz et al., 2007). The literature indicates strong alignment between risk and trust by both clients and vendors.

In the context of financial online banking systems, older people have a different perspective on risk than younger generations (Wilkowska, W., & Ziefle, M. 2009; Zheng, Spears, Luptak, and Wilby, 2015). In part this is because the risk is greater should an older person suffer financial loss and need to return to work to survive (Stark, Choplin, Mikels, and McDonnell, 2014). When older people are faced with decisions regarding online systems, their risk appetite is far less pronounced than that of others (Pew Research Centre, 2014).

Older people perceive inherent risk in internet banking and remain unconvinced of the need to change from existing trusted systems that are performing adequately and to the general satisfaction of older citizens (Littler and Melanthiou, 2006; ANPEA, 2008). Trust and risk are closely associated indicators in the determination of ICT acceptance (Kuriyan et al., 2010). In online banking terms, trust and risk inform acceptance through variables such as transaction viability, perceived risk, voluntary loss of privacy, mandatory loss of privacy, and reputation (Keat & Mohan, 2004; Pavlou, 2003). Online banking and associated financial transactions appear to draw out the strongest factors of influence against technology acceptance, in particular acceptance decisions that align with the pragmatics of money movements and financial security (Pavlou, 2003; Reisenwitz et al., 2007).
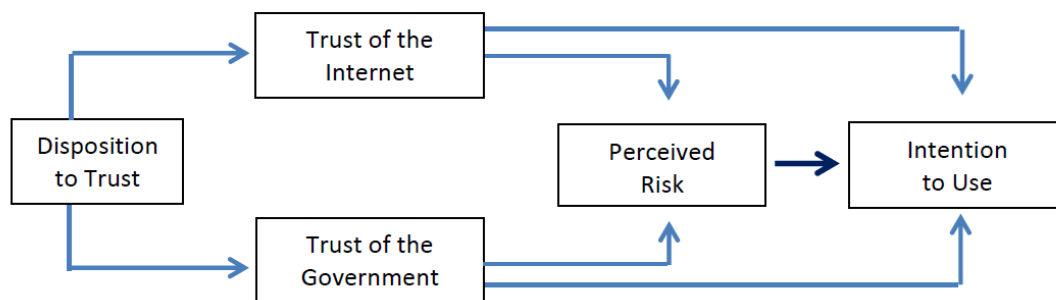
A Simple Trust and Risk model (T&R) adapted from Belanger et al. (2008)

Figure 2.9. Simple Trust and Risk Model

In e-commerce, perceived risk often translates to the rejection of an ICT (see Figure 2.9) and a decision about the intention to use or not to use a system (Belanger & Carter, 2008; Campbell et al., 2012). If a consumer is unsure about the security of the information required to complete a transaction, then the operation is often abandoned and the transaction remains incomplete (Pavlou, 2003). In transactions such as online shopping, an American Association of Retired Persons, (AARP) survey showed that older citizens held much less trust in online environments because they perceived a much higher level of risk, and a much lower level of control over the transactional process (Reisenwitz et al., 2007). In many cases of online shopping, the final transaction does not eventuate and the virtual shopping cart is abandoned before a purchase is made (Bizrate, 2000; Kuriyan et al., 2010).

As Figure 10 shows, there are two key features of the relationship between trust and risk in the standard TAM format. Whilst perceived risk can inform an intention to make an online transaction, as can Perceived Usefulness, (PU) and Perceived Ease of Use (PEOU), the far more important feature is the actual transaction. In the trust and risk-based TRTAM model (see figure 2.10) the *intention to transact* and the *actual transaction* are clearly the principal constructs. Here the literature shows the influence of the theory of reasoned action, where the TRA model made a similar distinction between *behavioural intentions* and *actual behaviour* (Davis et al., 1989).

There appears to be a much more pragmatic and direct relationship between trust and risk (Campbell et al., 2012). The perceived risk variable is stated as having a more galvanising effect than other variables on the acceptance of an ICT (Fairchild, 2003; Gan et al., 2006; Keat & Mohan, 2004;

Pavlou, 2003). Perceived risk is a combination of behavioural uncertainty and environmental uncertainty. The behavioural uncertainty is driven by the impersonal and reputational-neutral characteristics of many online service providers (Campbell et al., 2012; Pavlou, 2003). Their behaviour is unpredictable (Figure 2.10). At the same time, the online environment of the Internet is also volatile and erratic. Perceived risk therefore has a strong influencing effect over decisions to accept or reject ICT usage (Campbell et al., 2012).
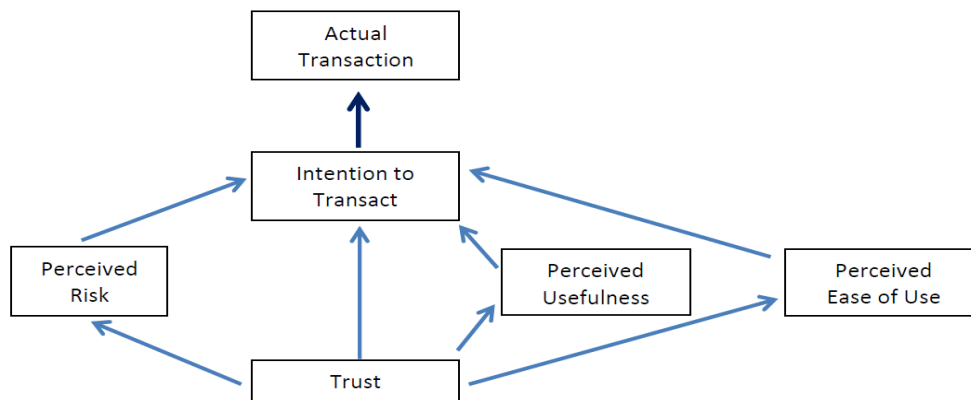
A TAM-based Trust and Risk model (TRTAM) adapted from Pavlou (2003)

Figure 2.10. A TAM-based Trust and Risk Model

2.7 Theories of Technology Acceptance and Usage

There are a range of different models that explain the take up of ICTs (see Figure 2.11). Some are based on perceptions whilst others use behaviours or needs to describe the acceptance (or rejection) of technology. The models included here are not an exhaustive list, but rather they are a representative sample of those models that the literature indicate have so far made the strongest impact on societies understanding of how technologies are acknowledged.

Diffusion Theory is the oldest of these theories, and is a launching platform for many of the other theories that start by asking how new ideas (in any format) are spread from one place to another. The largest collection of models is the Technology Acceptance models (TAM, TAM1, TAM2, TAM3, UTAUT, and STAM) which have dominated the literature based upon the two-pronged variables of "perceived usage" (PU) and "perceived ease of use" (PEOU). Cognitive Dissonance Theory (CDT and Task Technology Fit Model (TTF) both owe partial parentage to Diffusion Theory. CDT recognises that innovation complexities have a relationship with technology rejection, whilst TTF places a greater emphasis upon needs than perceptions.
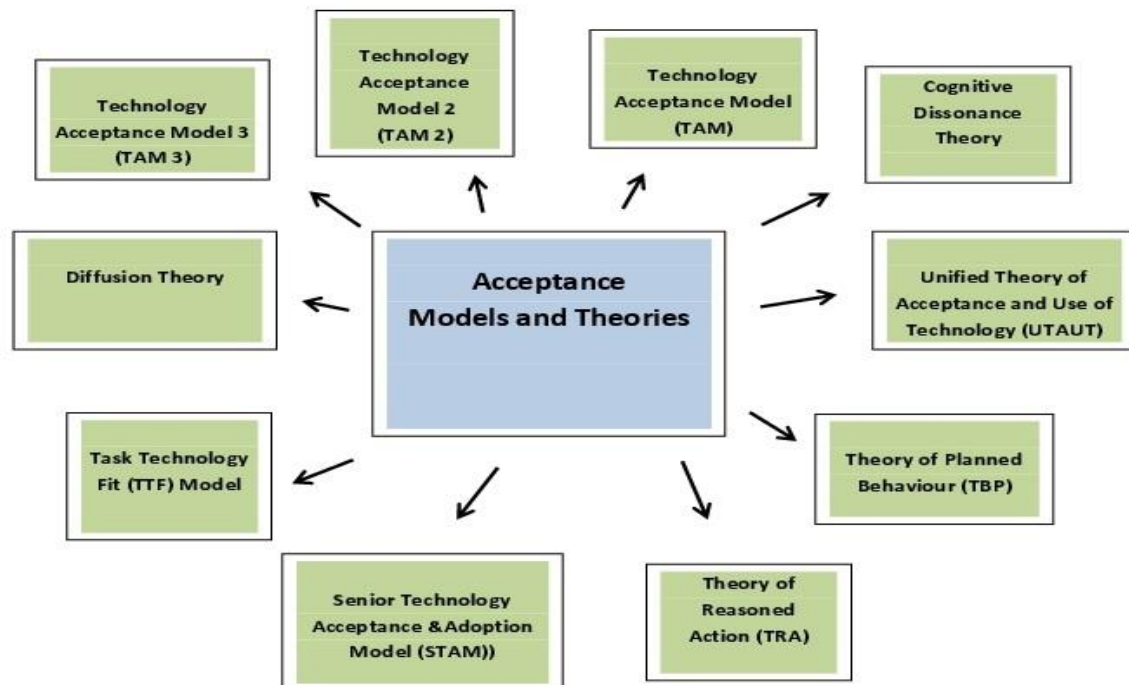
Figure 2.11. Acceptance Models and Theories

The Theory of Rational Action (TRA) and its derivative the Theory of Planned Behaviour (TPB) both rely on subjective norms. They acknowledge that technologies can be rejected, but they both place a heavy reliance on the cost of technology. TPB takes the normative theory further by considering financial factors in terms of actual behaviour. This next section explains their contributions in greater detail.

2.7.1 Diffusion, Complexity, and Adoption

The diffusion of technological advances is a useful discourse in a literature review of ICT acceptance, trust and usage because it attempts to explain the way new ideas (specifically those that relate to ICTs) spread through society (Venkatesh and Bala, 2008). The theory is applicable to human computer interaction (HCI) because it examines the process of communication of new ideas and innovations (Agarwal, Ahuja, Carter and Gans, 1998), in terms of the speed with which the innovations proliferate (Mitzner et al 2010), and the social elements that influence each new idea (Agarwal, Animesh and Prasad, 2009). As older people interact with ICT innovations, the ability to identify the rate of diffusion helps to explain the characteristics of ICT trust and usage.

This spread of diffusion has been described as a key measurement in the success or failure of an ICT innovation (Cody, Dunn, Hoppin and Wendt, 1999; Kenny and Milne, 2014). However, where it explains the acceptance in terms of its popularity the theory is an insufficient framework to independently explicate trust in terms of expectation, reliance and dependence (Choi and DiNitto, 2013; Cracknell, 2010). Diffusion theory has five main phases: awareness, interest, evaluation, trial, and adoption (Rogers, 2003). It is a generalist theory (see figure 2.12), claiming that ideas do not necessarily need to be innovative but rather they are perceived by others as original and inventive (Agarwal and Prasad, 1997; Venkatesh and Bala, 2008; Reneau, 2012). The diffusion takes place as a perceived innovation is socialised so that an individual is exposed to an innovation, is then persuaded to consider the innovation and then decides to try it (Singer, Baradwaj, and Rugemer, 2012: van Biljon and Kotz, 2007). Innovations that pose less risk are less problematic to implement as the prospective harm from failed assimilation is lower (Meyer and Goes, 1988).
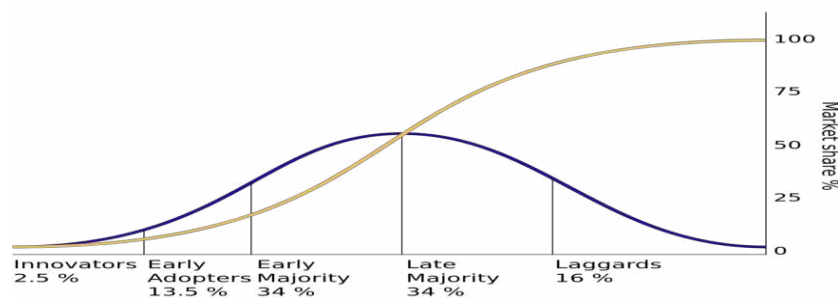
Figure 2.12. Rogers' Diffusion Curve adapted from Diffusion of Innovations (Rogers, 2003)

A different feature of diffusion is that of complexity. ICT trust and usage are both influenced by how difficult an innovation is to be understood (Rogers, Mayhorn, and Fisk, 2004). Rogers (2003, p288) posits that "the complexity of an innovation, as perceived by members of a social system, is negatively related to its rate of adoption." In this sense, new innovations and technologies might easily be mapped to a continuum, citing the relative complexity or simplicity of each new idea (Reneau, 2012).

This idea can extend to innovation users by considering the relative perspectives of early adopters versus stragglers (Cody, Dunn, Hoppin and Wendt, 1999; Russell, Campbell, and Hughes, 2008). In terms of ICTs, early adopters were programmers and people with ICT expertise (Virokannas, Rahkonen, Luoma, and Sorvari, 2000). Their perceptions of each new innovation were that they were easy to embrace.

In contrast, large numbers of older people are stragglers (Lee and Coughlin, 2014), who from a novice ICT viewpoint, see new ICT innovations as complex (Agarwal, Ahuja, Carter, & Gans, 1998; Rogers, 2003). Whilst this is useful in understanding complexity, it does not answer the issue of trust, and it only partially accounts for usage by older citizens (Chu, 2010). Early thoughts about technology change and innovation discuss the difference between rational choice (Kennedy, 1964) and counter-corresponding perceptions, desires and beliefs about technology (Ahmed, 1966; Nordhaus, 1973). The diffusion of innovation theory has been criticised not placing sufficient importance on the social constructions of how people accept technology (Lyytinen and Damsgaard, 2001; Choi and Ruona, 2010). The idea that innovations and technology changes can simply be accepted by everyone ignores the subjective manner in which people attempt to "make-sense" of something hitherto unknown or not yet fully understood (Rogers, 2003). These pieces of technical knowledge, experience and perception are elements of diffusion, and their absence demonstrate decision systems that appear to lack 'micro-foundations' (Elster, 1983). For both Elster and Rogers the process is an entirely changeable one that is based upon socio-cultural variables as well as perceptions, trust and confidence. It is inherently complex. There is recognition for the relevance of diffusion and innovation theories, however it remains open to criticism in its ability to explain reluctance to adoption in circumstances where imposed or mandated usage occurs. It puts forward a simplistic rationale citing risk and harm, but does not embrace the added complexities that social constructions infer.

One supporting theory that builds upon the idea of diffusion is cognitive dissonance (Purdie and Boulton-Lewis 2003). Cognitive Dissonance Theory (CDT) suggests that the more complex an innovation, the greater the chance that people will find other reasons to support their decision not to embrace that innovation (Elster, 1983). CDT offers another partial explanation for how new technology is trusted and/or used (Consolvo, McDonald, and Landay, 2009). However, CDT also clarifies that there is a need to distinguish between ICT usages and trust (Brown and Venkatesh, 2005). CDT understands and describes scenarios where ICT users do not trust the usage of innovations (Barker, 2000; Boulton-Lewis, 2010). Similarly, it is also possible to describe a person who might trust an innovation without having ever used it (Lagana, 2008). Attitudes and behaviours are described as influencing factors using CDT (Adali, 2013). Thus the complexity of an innovation can be perceived differently according to how it is used, if it is used, and even whether it is a suitable option to be considered for use (Thompson, Higgins, & Howell, 1994). The complexity of an innovation can therefore receive acceptance and/or usage based on whether it represents an appropriate fit between the task expected and the capabilities of the technology and the user of that technology (Summer, 2007). The literature on CDT is useful but limited to those imposed ICTs that are perceived as complex.

Others have sought to understand the complexity components of diffusion theory (Zmud & Apple, 1989). By looking beyond the process of implementation to include the vested interests of the stakeholders and the context in which an innovation is discovered, a number of factors emerge. The table below gives an indication of a segmentation that identifies the diffusion of innovations variables (Cooper & Zmud, 1990).

Table 2.2 An IT Implementation Diffusion Process. Adapted: (Zmud & Apple, 1989)

Variables	Processes
Initiation	*Scanning of problems and opportunities. Push (technological innovation) and Pull (organisational need) factors involved in decision to change*
Adoption	*Rational and Social negotiations begin – socialisation of a new idea.*
Adaptation	*Organisational procedures are developed and enhanced. Innovation able to be used.*
Acceptance	*Usage begins.*
Routinization	*Usage becomes a normal activity*
Infusion	*Optimisation and effective usage takes hold.*

Table 2.2 indicates a possible segmentation of variables. As an exemplar it is criticised as too simplistic to properly inform an understanding about the nuances of technology acceptance (and rejection) (Agarwal & Prasad, 1997). However, these variables form a starting point from which to derive a clearer understanding about how ICTs are accepted. Decisions that are made about IT usage and implementation are also dependent on what alternatives are available at the time, as well as what level of criticality aligns with each innovation usage (Goodman, 1986). The complexity of usage and trust is strongly connected with a range of variables that are uncertain (Cooper & Zmud, 1990). On the one hand diffusion theorists consistently note that an accepted technology or innovation needs to be compatible with its users and be suitable for the tasks that it is intended (Cooper & Zmud, 1990; Kimberly, 1981; Tornatzsky et al., 1983), on the other hand, decisions that are made about IT usage and implementation are also dependent on the risk appetite of the user (Rogers, 2003). To add to the ambiguity of understanding diffusion theory, Cooper and Zmud's process assumes that there is an order/process to the way in which usage of an ICT takes place. It does not consider the resistance to the way change can be imposed upon others (Fuegen and Brehm, 2004; Knowles and Linn, 2004, Choi and Ruona, 2010). Wynekoop, Senn, and Conger, (1992) suggest that it may work where technology acceptance occurs freely, but it does not account for usage that is mandated by others (Wynekoop, Senn, & Conger, 1992). Thus it is possible for an ICT user to routinely use an innovation before having rationally or socially accepted that usage (Agarwal & Prasad, 1997; Brown et al. 2002; Mendoza et al 2013).

One extension of diffusion thinking is centred on technology acceptance based around specific needs or tasks. The Task Technology Fit (TTF) theory suggests that IT usage is expected to be more meaningful in cases where the ICT innovation in use is matched in terms of both the task at hand and the capabilities of the innovative product (Goodhue & Thompson, 1995). The use of ICTs can be measured in terms of their efficacy. However, TTF (Figure 2.13) suggests that the way in which tasks are designed to be completed is more important than practicality and usefulness in determining expectations about a given technology's utilisation (Goodman and Thompson, 1995; Floyd and Zahra, 2007). Studies into usage of ICTs based upon fit are instructive where the acceptance of that technology is either incidental or voluntary (Thompson, Higgins, & Howell, 1991). TTF appears less conclusive

as a theory where the use of an innovation is either mandated or imposed (Benamati & Serva, 2007; Chan et al., 2010). The decision to use an ICT, whilst often successful where there is a fit between the task and the usage is, however, ostensibly influenced by other additional factors (Floyd and Zahra, 2007) such as social norms and behavioural attitudes (Thompson et al., 1991). The literature in this area is not well defined in terms of mandated ICTs, but it does point to the need for the inclusion of shared customs and activities.
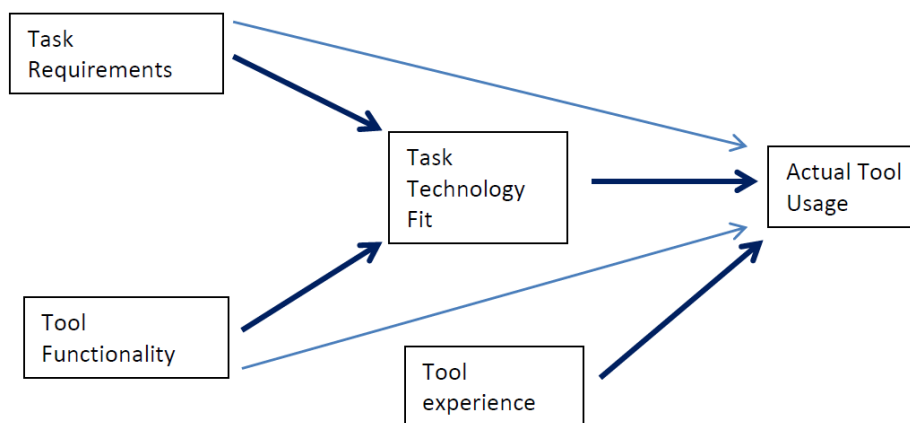
The Task Technology Fit (TTF)model adapted from Dishaw and Strong (1999)

Figure 2.13 The Task Technology Fit Model

Studies on the usage of personal computers place greater emphasis on social factors, cultural influences, and their corresponding habits, customs and practices (Fishbein & Ajzen, 1975; Thompson et al., 1994; Triandis, 1980). This inclusion of beliefs and perceptions is not intended to openly contest the task technology fit theory, but rather to incorporate a number of additional factors that assist in forecasting ICT choices. In this sense attitudes are a predictor of ICT usage (Robey, 1979). Social influences and societal norms impact on trust (Belanger & Hiller, 2006; Benamati & Serva, 2007; Chan et al., 2010). Thus the expected consequences from using ICTs are connected with both the user's individual perceptions, as well as those in their environment (Thompson et al., 1991; Triandis, 1980). The combination of 'Behavioural Intentions' (BI) and what Fishbein and Ajzen (1975) refer to as 'Subjective Norms' (SN) forms the basis of the Theory of Reasoned Action (TRA). Behavioural intention measures the strength of a person's intent on behaving in a certain manner. Subjective norms

describe "the person's perception that most people who are important to him think he should or should not perform the behaviour in question" (Fishbein and Ajzen 1975, p. 302).
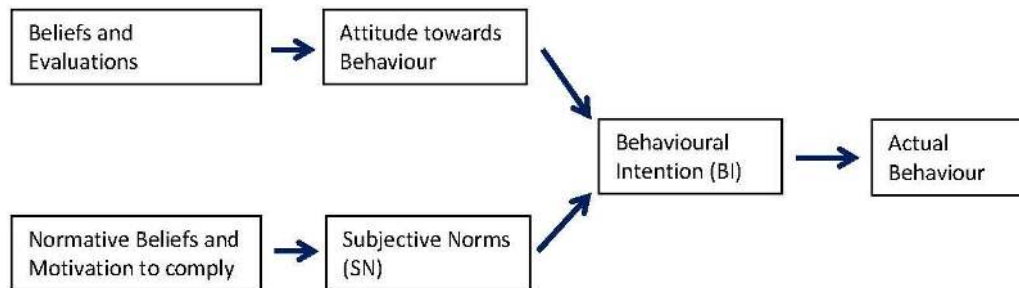
Theory of Reasoned Action (TRA) adapted from Davis et al (1989)

Figure 2.14. Theory of Reasoned Action Diagram

The Theory of Reasoned Action is an important milestone theory. It can assist in explaining and understanding some of the general areas about how computer technology usage decisions are made. TRA relies on the researcher identifying those normative beliefs that establish a set of subjective norms (Figure 2.14). This is a broad approach and requires the investigator to determine a set of salient beliefs that apply to a given sample population. Davis et al (1989) posit that TRA is advantageous in examining ICT usage because any factors not directly considered are still expected to influence results by way of their indirect influence to either behavioural attitudes or normative beliefs. Thus user acceptance of technology retains the inclusion of internal psychological variables as well as external norms and values. TRA has broad appeal but has been criticised for not fully accounting for elements of thrift and frugality that often accompany cost prohibitive perceptions of new technology (Hale, Householder, & Greene, 2002; Liska, 1984). Unlike other adoption models, the TRA fully acknowledges the likelihood of rejection as one of the expected outcomes of a rational decision about the adoption of a technology (Dalcher and Shine, 2003). TRA does not, however, provide a model that adequately allows for mandated or imposed technology adoption (Fuegen and Brehm, 2004; Knowles and Linn, 2004, Choi and Ruona, 2010).

A second derivative of the Theory of Reasoned Action is the Theory of Planned Behaviour (TPB) (Asjen, 1985). The TPB model took the previous TRA model and changed the emphasis from behavioural intention to actual behaviour (see Figure 2.15), in response to criticism about the inadequacy of the TRA model in determining outcomes where that behaviour was incomplete (Asjen, 2002; Sheppard, Hartwick and Warshaw, 1988). Whilst extending the TRA model to include actual behaviour, the TPB remains inadequate as a model that could explain or discern between mandatory, imposed, or voluntary acceptance of technology (Solomon, Russell-Bennett and Previte, 2012; Teo and Pok, 2003; Venkatesh, Morris and Ackerman, 2002). As in the case of the TRA, the issue of thrift and economic caution remains problematic in the TPB, particularly in the context of older people people who cannot afford to experiment with multiple and rapidly changing technology usage (Luarn and Lin, 2005). Whilst both TRA and TPB offer explanations for actions involving financial decisions, both remain inadequate in scenarios where there is low volition (Alsajjan and Dennis, 2010).
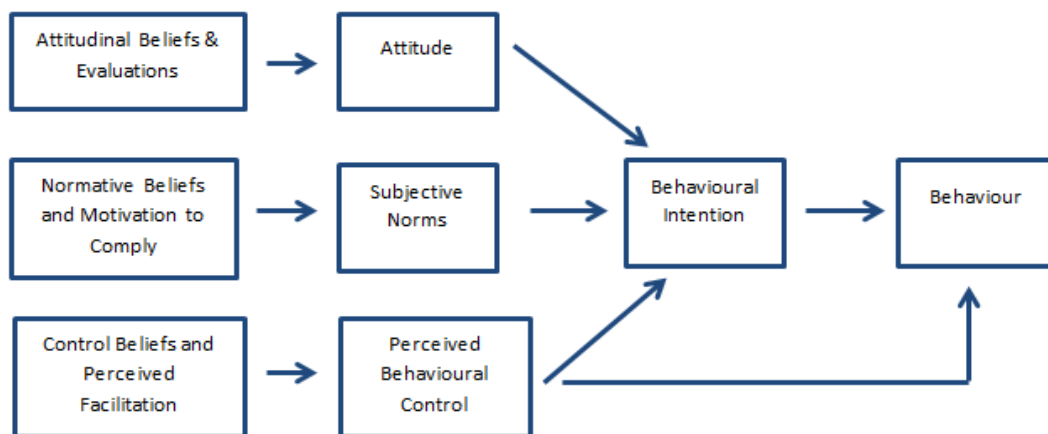
Theory of Planned Behaviour (TPB) adapted from Asjen 1985

Figure 2.15 Theory of Planned Behaviour (TPB)

2.7.2   Technology Acceptance Model (TAM)

In response to the issue of parsimony, frugality, and opportunity, limitations are regarded as important to the study of technology adoption since they can have a direct impact upon issues of trust and usage (Keat & Mohan, 2004). Partially as a response to these inadequacies, the Technology Acceptance Model (TAM) was introduced to more directly assist in the specific user understandings in the area of

information systems user acceptance (Davis, 1986). TAM allows for the tracking of specific beliefs and attitudes against the external factors that dynamically influence their affect upon the intended and actual use of information technology systems. To achieve this TAM (see Figure 2.16) suggests that there are two specific beliefs that directly influence ICT usage and activity (Davis, Bagozzi, & Warshaw, 1989). The *perceived usefulness* (PU) and the *perceived ease of use* (PEOU) determine attitudes and intentions that determine ICT usage. The *perceived usefulness* (PU) is a measure of the likelihood that an ICT usage will result in improved work performance (within a specific context). The *perceived ease of use* (PEOU) relates to a user's expectation about how easy and unproblematic a given ICT usage will be (within a specific context). The two variables PU and PEOU are dissimilar in the statistical sense, yet they are contextually connected to contrasting elements relating to usage (Davis et al., 1989).
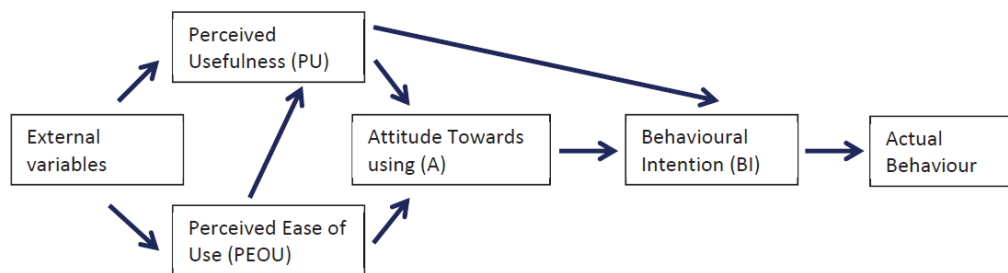
Technology Acceptance Model (TAM) adapted from Davis et al (1989)

Figure 2.16. Technology Acceptance Model (TAM)

Perceived usefulness and perceived ease of use both influence decisions about ICT usage directly. Davis et al (1989) posit that usefulness combined with the behavioural intention of an ICT user are both considerations that emerge based upon a rational and cogent judgment of how the usage will progress their activity.

> "*TAM theorises that the effects of external variables on intention to use are mediated by perceived usefulness and perceived ease of use. According to TAM, perceived usefulness is also influenced by perceived ease of use because, other things being equal, the easier the system is to use the more useful it can be.*" (Venkatesh & Davis, 2000)

TAM moves beyond TRA in that it does not solely attempt to acquire numerous subjective norms in order to determine behavioural intentions. TRA is a model that is suited to explaining volitional behaviours (Ajzen, 1985; Bentler & Speckart, 1979), whereas TAM embraces additional choices that include various types of coercion (Davis et al., 1989). In this sense TAM allows for the inclusion of intentional usage that might, for example, be mandated by circumstance. TRA is considered a weaker model than TAM in attempting to include decisions about trusted usage because it does not allow for those intended usages that are imposed (Davis, 1986). In specific terms of ICT usage, TRA has also been criticised for instances where "subjective norms" can be influenced by the attitudes of others to possibly form a "false consensus" relating to normative beliefs (Hale et al., 2002).

TAM treats perceived usefulness (PU) as a more important variable than attitude (Davis et al., 1989). TRA has also been criticised as an inferior model in terms of mandated practices. The grouping of variables known as "subjective norms" (SN) does not discriminate between imposed compliance and voluntary adoption (Warshaw, 1980). Thus usage that is decreed from a supervisor may ignore the user's own set of beliefs about any given ICT application and may infer deference towards the beliefs and attitudes of others (Oliver & Bearden, 1985). This makes TRA an unsuitable model in its own right to test for trust in ICT usage (Xin, Valacich, & Hess, 2004). TRA is, however, a useful stepping stone towards a model that more specifically allows measured acceptance for both mandatory and voluntary ICT usage. Both TAM and TRA share the assumption that usage attitude is decided using one's norms and beliefs (Davis et al., 1989), but differ where TRA sums all beliefs together whilst TAM looks to two main beliefs (PU and PEOU) that are treated as separate constructs.

Contemporary ICT innovations are increasingly connected with self-efficacy through one's perceived ease of use (PEOU). The easier a system can be engaged with, the greater one's ability to progress the ongoing interaction (Bandura, 1982). The effect of hardware such as a mouse or a touchscreen, combined with software additions such as menus and icons, represent milestone achievements that strengthen self-efficacy in ICT usage (Lam, & Lee, 2006; Wilkowska & Ziefle, 2009). Thus there are two factors by which PEOU can influence usage behaviour. The first is the value of the efficacy by which usage is intuitive and natural (Cook et al., 2011a; John & Sutherland, 2004;

Savenstedt, Sandman & Zingmark, 2006).   This applies to elements where usage commences irrespective of prescriptive instruction or training. The second set of factors is the instrumental components that allow for faster, crisper, brighter, or more thorough elemental usage (Wong, 2011).

Of significance in understanding utilisation is the relationship between complexity and usage. If a new ICT is perceived as complex to use, the interest in usage often has an inverse relationship to its acceptance (Davis et al, 1989). Thus, where TAM proponents posit that PU and PEOU positively affect user attitudes (Davis, 1986; Schultz & Slevin, 1975) usage that shows complexity has a negative effect on user attitudes (Venkatesh, 2000). Perceived ease of use is a complex construct that can be shaped by many variables. Greater levels of complexity reduce the effectiveness of incorporating PEOU. The over simplicity of the PU and PEOU descriptors are unhelpful when attempting to understand a model that incorporates the differences between mandated, imposed, and voluntary adoption of technology (Jackson, Chow and Robert, 1997; Adams, Nelson, and Todd, 1992; Brown, Massey, Montoya-Weiss and Burkman 2002; Venkatesh 2000, Ram and Jung, 1991).

2.7.3   Technology Acceptance Model 2 (TAM2)

After many studies over a considerable time-span TAM has become accepted as a reliable predictor of user acceptance in ICT (Bagozzi, 2007; Venkatesh & Davis, 2000). Despite this consistency there are other contributing factors beyond the original model that influence usage. TAM2 extends beyond the original TAM to include additional constructs that include subjective norms, voluntariness, image, job relevance, output quality, result demonstrability, and perceived ease of use (Figure 2.17). The first three of these additions are interrelated social forces whilst the remaining four additions are cognitive instrumental processes.

The inclusion of subjective norms as a determinant of usage is a consistent with earlier work on the Theory of Reasoned Action (TRA) (Fishbein & Ajzen, 1975). People may elect to behave in one way even though they are not personally drawn towards acting in such a manner. This is best represented by two other conditions. The first is that users perceive that others of importance think that they should behave in such a way, and the second is that they are inclined to conform to those other people (Ajzen, 1991). TAM proponents have since conceded that social influences affect usage behaviour (Venkatesh & Davis, 2000).

Of specific interest to the understanding of trusted usage by older people is the difference between voluntary and mandatory circumstances. Specifically, TAM2 attempts to address subjective norms where mandatory settings are in play. TAM2 theorises that compliance occurs where an individual executes behaviour in order to attain a specific recompense or to avoid a specific penalty (Venkatesh & Bala, 2008). Differences in subjective norms were noted between mandatory usage (where the subjective norms influenced acceptance) and voluntary usage (where no such influence was apparent (Harwick & Barki, 1994). Thus TAM2 posits that in mandatory ICT usage there is additional influence over and above the two determinants known as perceived usefulness (PU) and perceived ease of use (PEOU). This has been extended to include internal and external organisational mandates (Hartwick & Barki, 1994). (Hartwick & Barki, 1994).
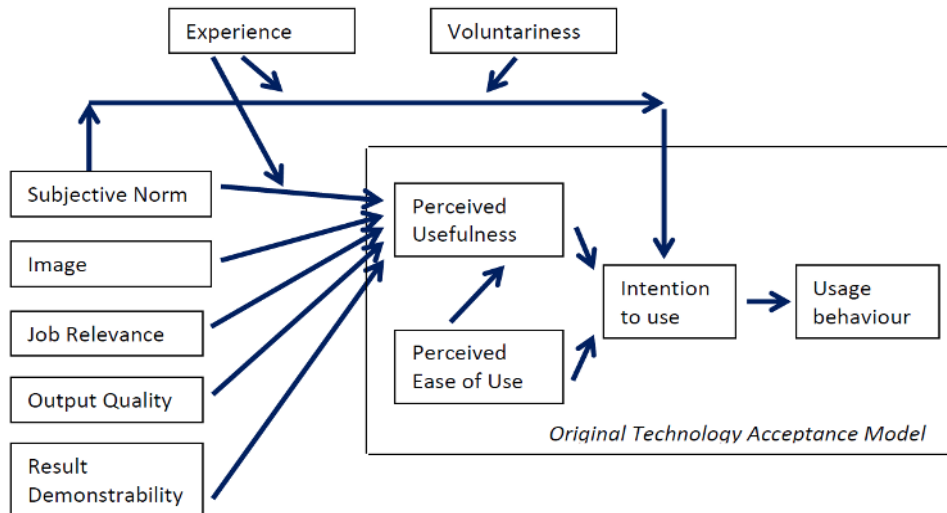
Technology Acceptance Model 2 (TAM 2) adapted from Venkatesh et al. (2000)

Figure 2.17 Technology Acceptance Model 2 (TAM 2)

The distinction between mandatory and voluntary contexts presents through the acceptance of subjective norms. Where (PU) and (PEOU) are measured, TAM2 also considers "voluntariness" as an influencing factor described as "the extent to which potential adopters perceive the adoption decision to be non-mandatory" (Hartwick & Barki, 1994). This variable is also described when addressing mandatory usage in the literature as "compliance" (Bagozzi, 2007; Chan et al., 2010; Venkatesh & Davis, 2000; Venkatesh et al., 2003).

The extended model (TAM2) also includes other specific subjective norms. TAM2 includes the influence of 'image'. It assumes that the subjective norm will positively influence image because where there are significant members of a person's community group who consider that a person should make use of an ICT then that usage will probably lift up that person's reputation and esteem within the community. TAM2 adds another variable to this consideration, positing that whilst a person complies with a mandatory usage (or one undertaken through the influence of image and expected esteem), that such subjective norms have a reduced effect "over time" (Venkatesh & Bala, 2008). Thus the initial mandating of a usage may assist a person to engage with ICT usage at the beginning, but that after gaining experience "over time" that user may revert to PU and PEOU (Agarwal & Prasad, 1997; Hartwick & Barki, 1994).

Another addition to TAM2 (from the original model), is a user's understanding of 'job relevance'. The original TAM model drew criticism from researchers who suggested that TAM had a lack of task focus (Dishaw & Strong, 1999). Perceived usefulness (PU) implied that a task was useful, but did not explain properly whether that usefulness had a direct influence on usage or whether it was specifically useful for the given task at hand. TAM2 draws elements from task Technology Fit (TTF) theory by suggesting that where usage is related to how applicable it is to the completion of tasks there is cognitive judgement by the user as to the personal relevance and job importance that corresponds with that usage (Goodhue & Thompson, 1995; Hartwick & Barki, 1994).

Venkatesh et al. (2000) posit that job relevance will have a positive effect on perceived usefulness. TAM2 also considers 'output quality' and 'result demonstrability' as influencing factors. It posits that people will bear in mind how well a system performs given tasks and consider the quality of outputs as a rationale for perceived usefulness. This element of TAM2 has strong connectivity with diffusion theory. In many instances this judgement is made on the basis of individual and commercial profitability (Agarwal et al., 1998).

2.7.4 Technology Acceptance Model 3 (TAM3)

The more recently considered model of technology acceptance is the Technology Acceptance Model 3 which seeks to differentiate from previous TAM iterations by attempting to qualify a '*lack of actionable guidance'* (Venkatesh & Bala, 2008). In putting forward TAM3, Venkatesh and Bala acknowledge that both the TAM and TAM2 were only capable of generalised identification of the two influencing determinants PU and PEOU. In a practical sense ICT usage might be developed with a TAM-based instruction to ensure that a given innovation was both useful and easy to use. The TAM3 model accepts that such a scenario is overly simplistic, and that whilst it night be obvious to include PU and PEOU in its development, it is a far more complex instruction that attempts to qualify how easy and how useful an innovation might become. Whilst one might crave an innovation that was easy to use but extremely useful, rather than a different product that was reasonably useful but extremely easy

to use, the more complex consideration is to ask whether the variables of PU could influence PEOU and/or could the variable of PEOU influence PU.

In order to better separate the elements of the construct PEOU, Venkatesh and Bala developed six determinants of PEOU (see Table 2.3). These determinants have an influencing relationship with PEOU in such a way that they can be added together with other determinants on the TAM2 model. This means that the social influence processes that were fundamental to assisting our understanding of perceived usefulness (PU) are not affected by the new addition of determinants that influence perceived ease of use (PEOU) (Venkatesh & Bala, 2008).

Table 2.3 PEOU determinants from Technology Acceptance Model 3

Determinants	Definitions
Computer Self-Efficacy	*The degree to which an individual believes that he or she has the ability to perform a specific task/job using the computer*
Perception of External Control	*The degree to which an individual believes that organizational and technical resources exist to support the use of the system*
Computer Anxiety	*The degree of "an individual's apprehension, or even fear, when she/he is faced with the possibility of using computers"*
Computer Playfulness	*the degree of cognitive spontaneity in microcomputer interactions"*
Perceived Enjoyment	*The extent to which "the activity of using a specific system is perceived to be enjoyable in its own right, aside from any performance consequences resulting from system use"*
Objective Usability	*A "comparison of systems based on the actual level (rather than perceptions) of effort required to completing specific tasks"*

PEOU determinants from Technology Acceptance Model 3 (Venkatesh and Bala, 2008).

Perceived Ease of Use (PEOU) is closely associated with an individual's self-efficacy beliefs, as well as their technical understanding (Davis et al., 1989; Venkatesh et al., 2003). Hands-on experience is required to determine PEOU. Venkatesh (2000) posited that people judge their PEOU by linking their perceptions to general beliefs about ICTs and then later altering their opinions based on their own applied practice with a specific innovation. Thus the first four ICT determinants in the table above (computer self-efficacy, perceptions of external control, computer anxiety, and computer playfulness) form 'anchors' in the form of characteristics and emotions that relate to ICT usage. The Technology Acceptance Model 3 also states that these determinants will not influence perceived usefulness (Chuttur, 2009).
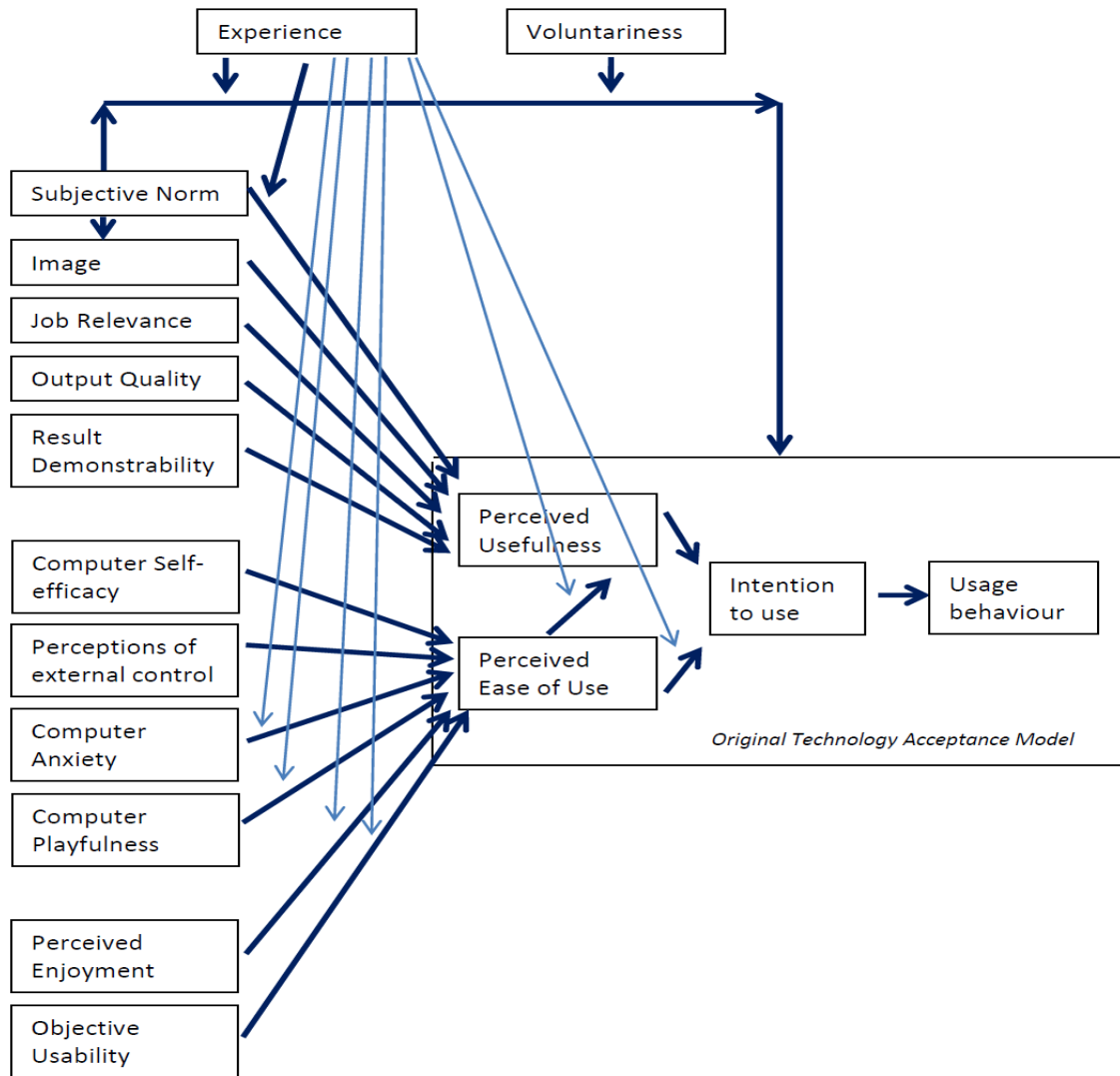
Technology Acceptance Model 3 (TAM 3) adapted from Venkatesh et al. (2008)

Figure 2.18. Technology Acceptance Model 3 (TAM 3)

The importance of applied practice in the form of hands-on usage is emphasised in TAM3, (Table 2.3), because TAM3 theorises that there is a transfer of behavioural attitude from PEOU to PU that takes place "over time" (Figure 18). The four 'anchors' of PEOU will change as more experience is acquired. This explains why 'experience' box in the TAM3 diagram is linked to both the subjective norms that influence perceived usefulness, but also several elements that influence perceived ease of use (Venkatesh & Bala, 2008). The theory of anchoring and its moderating effect "over time" is independently supported by others (Mussweiler & Strack, 2001).

The TAM3 model suggests that 'experience' will moderate the effect of computer anxiety on PEOU. As experience increases "over time" the effect of computer anxiety on PEOU will diminish. Simultaneously as applied practice increases so too will the strength of the determinants objective usability and perceived enjoyment grow "over time". Venkatesh et al (2008) refer to perceived enjoyment and objective usability as adjusting information variables. They posit that not only is perceived ease of use moderated by experience on an individual basis, but that as anxiety declines "over time" objective usability and perceived enjoyment through experience allow users to make more accurate perceptions about how long each usage might take, how much effort is required, and how complex each usage might be. The notion that voluntary experience would reduce the anxiety connected with PEOU "over time", whilst mandated usage would retain a stable set of perceptions, has been used as a comparator for trust (Venkatesh & Bala, 2008). However, trust is more complex than simply measuring voluntary usage over an extended period of time. The TAM3 model still fails to demonstrate an understanding of trust in instances where the usage has been imposed.

2.7.4.1   Summary of TAM models and iterations

The Technology Acceptance Model has a number of limitations. TAM has a prominent status that is derived from its associations with diffusion theory, the theory of planned behaviour, and the theory of reasoned action. Its two main behavioural influencers are the Perceived Ease of Use (PEOU) and Perceived Usefulness (PU). However, a strong criticism of TAM is that these two influencing factors make for an overly simplistic model to account for a variety of measures, behaviours, reactions, and perceptions (Bagozzi, 2007). On the one hand researchers extol the succinctness of TAM for asserting that no more causes or forces of behaviour should be assumed than are necessary to account for the facts, yet on the other hand researchers acknowledge the progressively multifaceted iterations of TAM, TAM2 and TAM3 that emerge with each new model. The introduction of new TAM determinants are an attempt to help explain the inability of the original TAM model to account for a more comprehensive reality that includes factors such as mandatory, obligatory, and imposed requirements to use and accept new technologies.

Further inconsistencies become visible when distinguishing between the usage intentions of an individual and those of someone allied to a group. A group member is subject to a variety of influencing determinants by comparison to an individual user. In reality there are very few usages that might be attributed to "single user" acceptance. Acceptance and usage is clearly influenced by other factors such as social identity, belongingness, collective esteem, and imposition (Bagozzi & Lee, 1999). Subsequently the need for a model that went beyond TAM resulted in the development of the UTAUT model (Venkatesh and Davis 2000).

2.7.5 Unified Theory of Acceptance and Use of Technology (UTAUT)

In 2003 Viswanath Venkatesh led a group of technology acceptance researchers to develop a more 'variable-laden' model of ICT acceptance. The UTAUT model is a technology acceptance model that aims to go beyond TAM frameworks by explaining in more detail user intentions and subsequent user behaviour. UTAUT posits that there are four main concepts (described as performance expectancy, effort expectancy, social influence and facilitating conditions), that are direct determinants of usage intention and action (Venkatesh et al. 2003). The theory suggests that gender, age, experience, and voluntariness of use can moderate the influence of the four main concepts of usage intention and action. The theory was developed as part of a review of previous models that had been used to explain usage acceptance. UTAUT draws from elements within the theory of reasoned action (TRA), the technology acceptance models 1 and 2 (TAM), the theory of planned behaviour (TPB), personal computer usage, the diffusion of innovations theory (IDT), and social cognitive theory. Hence the notion of a unified theory has been put forward. UTAUT claims to deliver a framework that better explains interdependencies, deeper and richer dynamic influences, and a better defined set of core constructs.
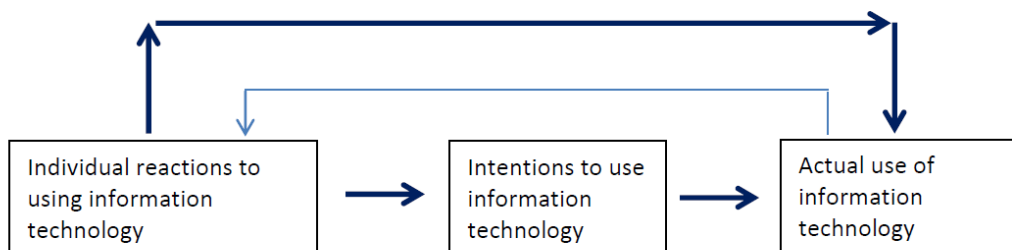
Basic Concept underlying User Acceptance Models, adapted from Venkatesh et al. (2003)

Figure 2.19. Basic concept underlying User Acceptance Models

One reason for a review of acceptance models (and the subsequent support for a unified model) was that none of the previous models appeared to deliver sufficient consistency across a range of previously non-aligned variables. The initial observation from UTAUT (Venkatesh et al, 2000) is to acknowledge a much more simplified representation of user acceptance (Figure 2.19). Venkatesh et al

(2003) acknowledge the earlier work surrounding the Task Technology Fit model (TTF) but note that the UTAUT model is grounded on the underlying principle that technology usage should be the single overriding dependent variable that remains across any unified approach.

The development of the unified model used this underlying principle as the footing for a different model that aimed to incorporate positive correlations from across the various user acceptance models previously described. Using a combination of longitudinal data from across a variety of studies, Venkatesh et al (2003) determined that there were seven constructs that demonstrated direct alignment with determinants of intention or usage across different models (Figure 2.20). From these results the four constructs of *performance expectancy*, *effort expectancy*, *social influence*, and *facilitating conditions* became the main determinants, whilst *attitude towards using technology*, *self-efficacy*, and *anxiety* were theorized as not having direct influence on intention or usage.
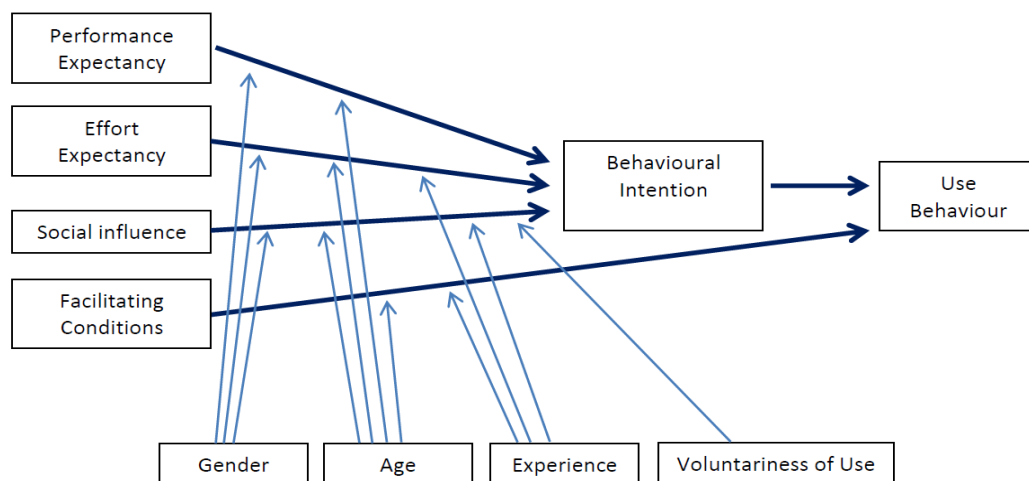
Unified Theory of Acceptance and Usage of Technology (UTAUT), adapted from Venkatesh et al. (2003)

Figure 2.20. Unified Theory of Acceptance and Usage of Technology (UTAUT) model

Compared with previous TAM iterations, the UTAUT model allows for a greater number of dynamic variables set against a single overriding dependent variable. The four key determinants shown on the left side of the UTAUT model play key roles in the prediction of usage and intended usage of ICTs.

Performance expectancy is posited as the degree to which an individual believes that using the system will help that individual to reach advances in job performance. This first construct is similar in many respects to the PU of TAM and TAM2, the job fit related to PC usage, the relative advantage of diffusions theory and the usefulness of the theory of planned behaviour. This construct is moderated by the variables gender and age. According to Venkatesh et al, (2003) it is the strongest predictor of intended usage.

Effort expectancy is advanced as the degree of ease associated with ICT usage. This construct can be associated with the PEOU from TAM and TAM2, complexity from PC usage, and ease of use from diffusion innovations theory (IDT). This construct applies in both voluntary and mandatory settings, but with the understanding that the significance decreases as usage is continued. This construct is moderated by the variables gender, age and experience. Based on the review of previous usage modelling, Venkatesh et al (2003) hypothesise that this construct is the strongest determinant in terms of gender and age, as related to previous technology acceptance work (Agarwal & Prasad, 1997; Davis et al., 1989; Thompson et al., 1994; Venkatesh, 2000).

Performance expectancy is posited as the degree to which an individual believes that using the system will help that individual to reach advances in job performance. This first construct is similar in many respects to the PU of TAM and TAM2, the job fit related to PC usage, the relative advantage of diffusions theory and the usefulness of the theory of planned behaviour. This construct is moderated by the variables gender and age. According to Venkatesh et al (2003) it is the strongest predictor of intended usage.

Effort expectancy is advanced as the degree of ease associated with ICT usage. This construct can be associated with the PEOU from TAM and TAM2, complexity from PC usage, and ease of use from diffusion innovations theory (IDT). This construct applies in both voluntary and mandatory settings, but with the understanding that the significance decreases as usage is continued. This construct is moderated by the variables gender, age and experience. Based on the review of previous usage modelling, Venkatesh et al (2003) hypothesise that this construct is the strongest determinant in terms of gender and age, as related to previous technology acceptance work (Agarwal & Prasad, 1997; Davis et al., Thompson et al., 1994; Venkatesh, 2000).

Social influence is posited as the level at which a person identifies that significant others believe he or she should use a new ICT. This construct is closely associated with the subjective norm of TRA, TAM, TAM2 and TPB. It is also allied with the social factors in PC usage and the construct of image in innovations diffusion theory. This construct does not respond to voluntary situations; however, it is an active determinant when usage becomes imposed or mandated. It is moderated by all four of the shown variables: gender, age, experience, and voluntariness of use.

Facilitating conditions is described as the level to which a person believes that an organisation and system infrastructure exists to maintain and operate the use of a given ICT. This construct is closely associated with the perceived behavioural control of TPB, the facilitating conditions outlined in the theory of PC usage, and the compatibility of IDT. The construct is moderated by age and experience. One of the strengths of the UTAUT model is that it allows research to understand technology acceptance and usage changes "over time". This is particularly interesting to studies that examine the actions and intentions of novice users as well as comparisons about dynamics associated with age (Venkatesh & Bala, 2008).

The unified theory of acceptance and usage of technology has received criticism for the large number of independent variables that can be considered. The UTAUT model integrates forty-one (41) independent variables for calculating intentions and also depicts eight (8) independent variables for calculating behaviour (Bagozzi, 2007). The model has been described as disorderly in its approach to logically presenting variable interaction and influence (Williams, Rana, Dwivedi, & Lal, 2011). The model has also been cited for its inability to consistently address parsimony (van Raaij & Schepers, 2008). Despite these criticisms, UTAUT is a popular choice of researchers investigating linkages between older citizens, technology acceptance and trusted systems (Al Awadhi & Morris, 2008; Gupta et al., 2008; Niehaves & Plattfaut, 2010).

2.7.6   Trust and Acceptance Model Timeline and Progression

The emergence of each new trust and acceptance model owes something to its predecessors. The models are derivative and each new model attempts to account for the gaps, limitations and inconsistences of previous models. Thus, since 1957 there have been a range of trust and acceptance

models that have emerged to meet the need to understand the trusted usage and acceptance of technology. He timeline provided (see Figure 2.21) shows the progression of the early models of Cognitive Dissonance Theory (1957 and the Diffusion of Innovation Theory (1962) through to 2008 and including the derivative Seniors Technology Acceptance and Adoption Model (STAM).
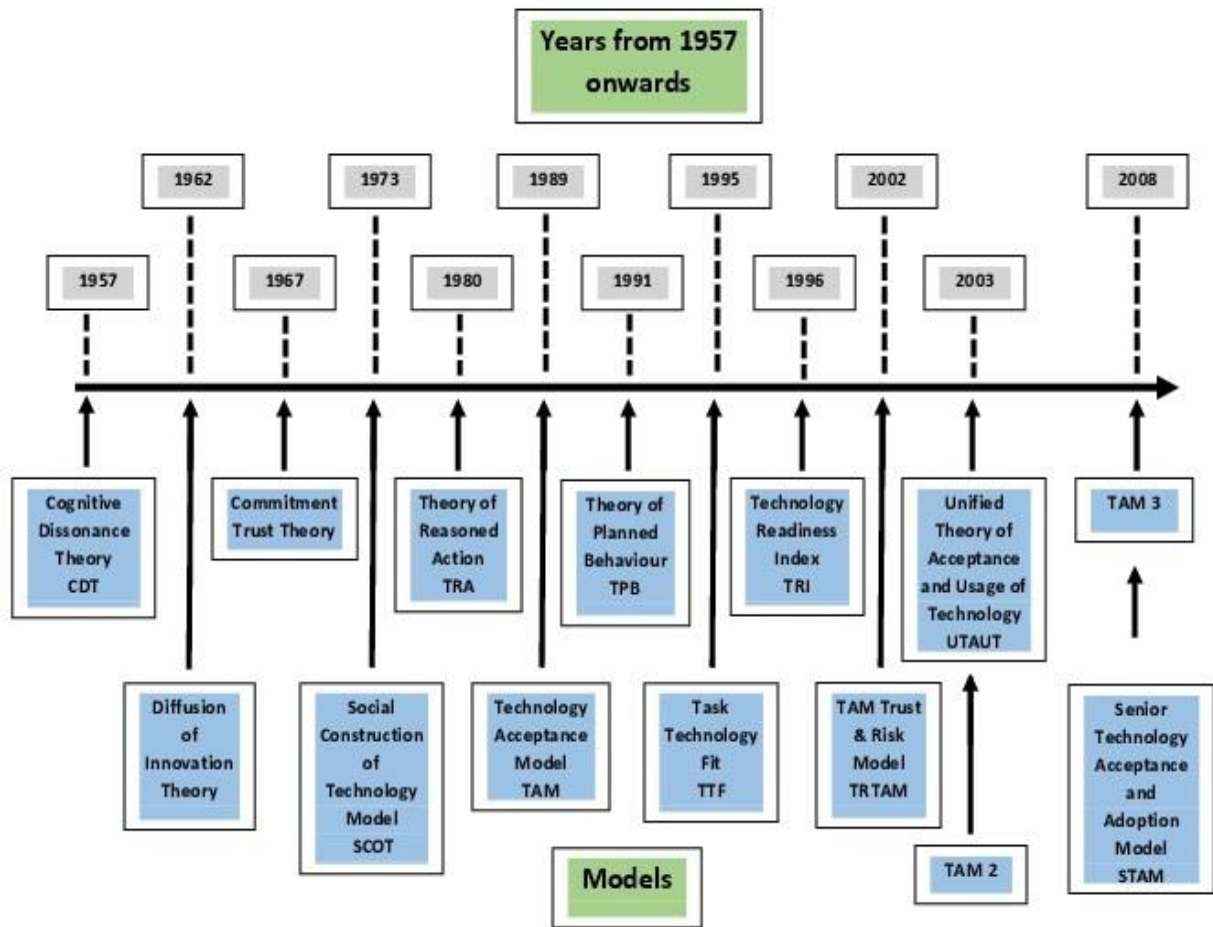
Figure 2.21. Timeline of Trust and Acceptance Models

2.7.7 Senior Technology Acceptance & Adoption Model (STAM)

With the inadequacies of TAM models to address the rejection of technologies by late adopters and laggards, particular versions of TAM have evolved to help describe the specific needs of subsets, such as older people (Mendoza et al, 2013). Previous acceptance models have generalised about the full range of potential users, often differentiating between early adopters and late adopters (Agarwal et al., 1998; Morris & Venkatesh, 2000). There is a need for a version of TAM that addresses the specific variable strengths that apply to older people. An alternate way to consider usage is to differentiate between *adoption* and *acceptance* of an ICT innovation. On the one hand technology adoption is best described as a process (Rogers, 2003), typically described as a progression starting with awareness and ending with actual usage of an innovation (Renaud & van Biljon, 2008), whilst on the other hand, acceptance describes an attitude rather than a process (van Biljon & Lotz, 2007). These attitudes can be influenced by a wide variety of factors (Bagozzi, 2007), whereas an imposed or mandated adoption of an ICT may only be enforced from one or two factors (Reneau, 2012).

The Senior Technology Acceptance & Adoption Model (STAM) looks more closely than other TAM variants at the adoption process for ICT innovations (Renaud & van Biljon, 2008). The model draws its basis from two differing views of adoption process. The first is derived from Rogers "Diffusion of Innovations" (2003) which defines a five stage process for innovation adoption (Table 2.4).

Table 2.4. Five stage adoption process Diffusion of Innovations (Rogers, 2003).

Phase	Description
Knowledge Phase	Where the person gets to know about the product
Persuasion Phase	Where the person becomes persuades of the need for the product
Decision Phase	Which leads to purchase or ownership
Implementation Phase	Where the item is used
Confirmation Phase	Where the individual seeks to confirm making the right decision in purchasing the product.

The second process draws from an understanding of users as social entities under the descriptor '*domestication of technology'* (Table 2.5). It is considered more applicable to older users (Renaud & van Biljon, 2008) because it allows for rejection (in addition to acceptance and non-acceptance) under a range of socially contextual variables (Silverstone & Hadden, 1996).

Table 2.5. Domestication of technology adoption process (Silverstone et al, 1996)

Dimension	Description	Themes
Appropriation	**Process of possession or ownership of the innovation**	**Motivation to buy a product**
Objectification	**Process of determining roles the product will play**	**Meaning of a technology**
Incorporation	**Process of interacting with a product**	**Difficulties in using a product (usability problems) Learning the process (instruction manual)**
Conversion	**Process of converting technology to intended feature use or interaction**	**Unintended use of product features. Unintended way of user interaction, Wishes for future products**

The STAM model incorporates a number of seniors' adult contexts in terms of social influence. Use of a mobile phone for example, might be different if the phone needs were critical to services such as emergency and health support as opposed to commonplace communications (Lee, 2007). Older people would have a different set of values towards the notion of communications and safety than others general age groups (Renaud & van Biljon, 2008). The social context is reasoned as significant in STAM because as people enter into senior citizenship their activities and involvement with others goes into decline (Levasseur, Richard, Gauvin, & Raymond, 2010).

STAM is similar to UTAUT insomuch as they both omit attitude as a determinant of distrust, influence, and technology rejection (Renaud & van Biljon, 2008). In a study of older people's acceptance of mobile phone technology, those participants who were dissatisfied with the ease of use of their phone still cited their intention to use the phone, because the context-based social influences were too strong to be offset by a phone that was difficult to use. Renaud and van Biljon (2008) claim that the area of strongest impact was phone usage. It led to the eventual acceptance of the innovation

(Renaud & van Biljon, 2008), however it did not clearly establish that the usage equated to trust under these conditions. STAM provides a clearer understanding of the process from adoption to acceptance, however the model does not specifically account for ongoing trust and mistrust (Figure 2.22). It assumes that once accepted through continued usage that the innovation is trusted.

Senior Technology Acceptance & Adoption Model (STAM) adapted from Renaud et al. (2008)
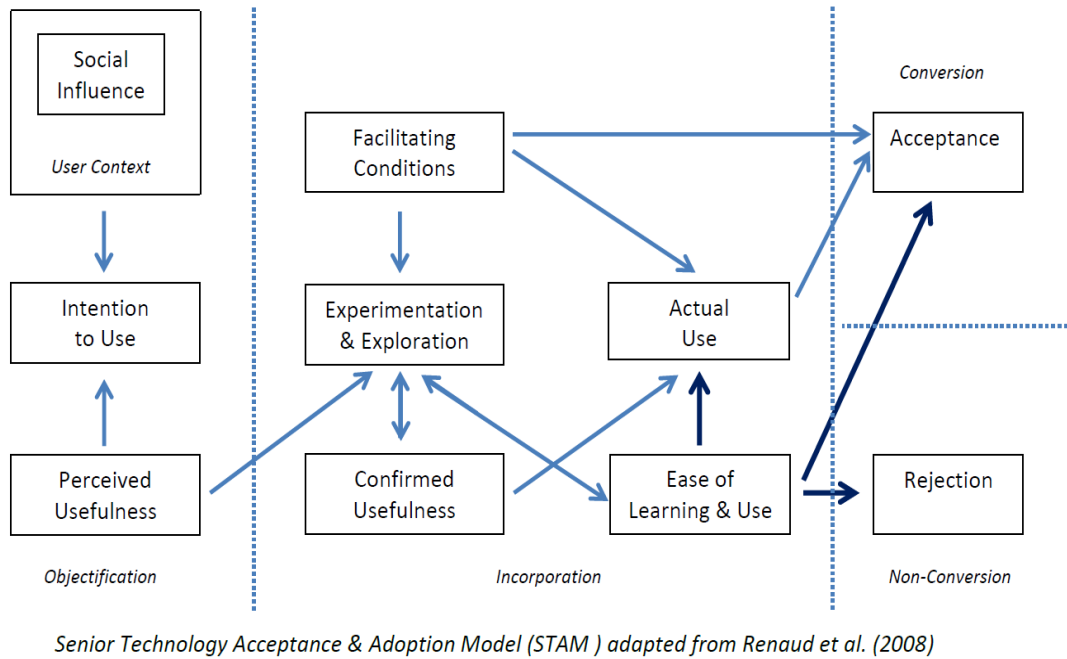
Figure 2.22. Senior Technology Acceptance and Adoption Model (STAM)

2.8   Summary of conclusions from the literature

By focusing on the literature that responded to trust, ICT innovation challenges, and older people, and by using a systematic approach to drill down to specific areas a clear picture emerges about the literature on ICT trust, and on the particular areas where there are gaps, confusion, and contestation of ideas (Figure 2.23).
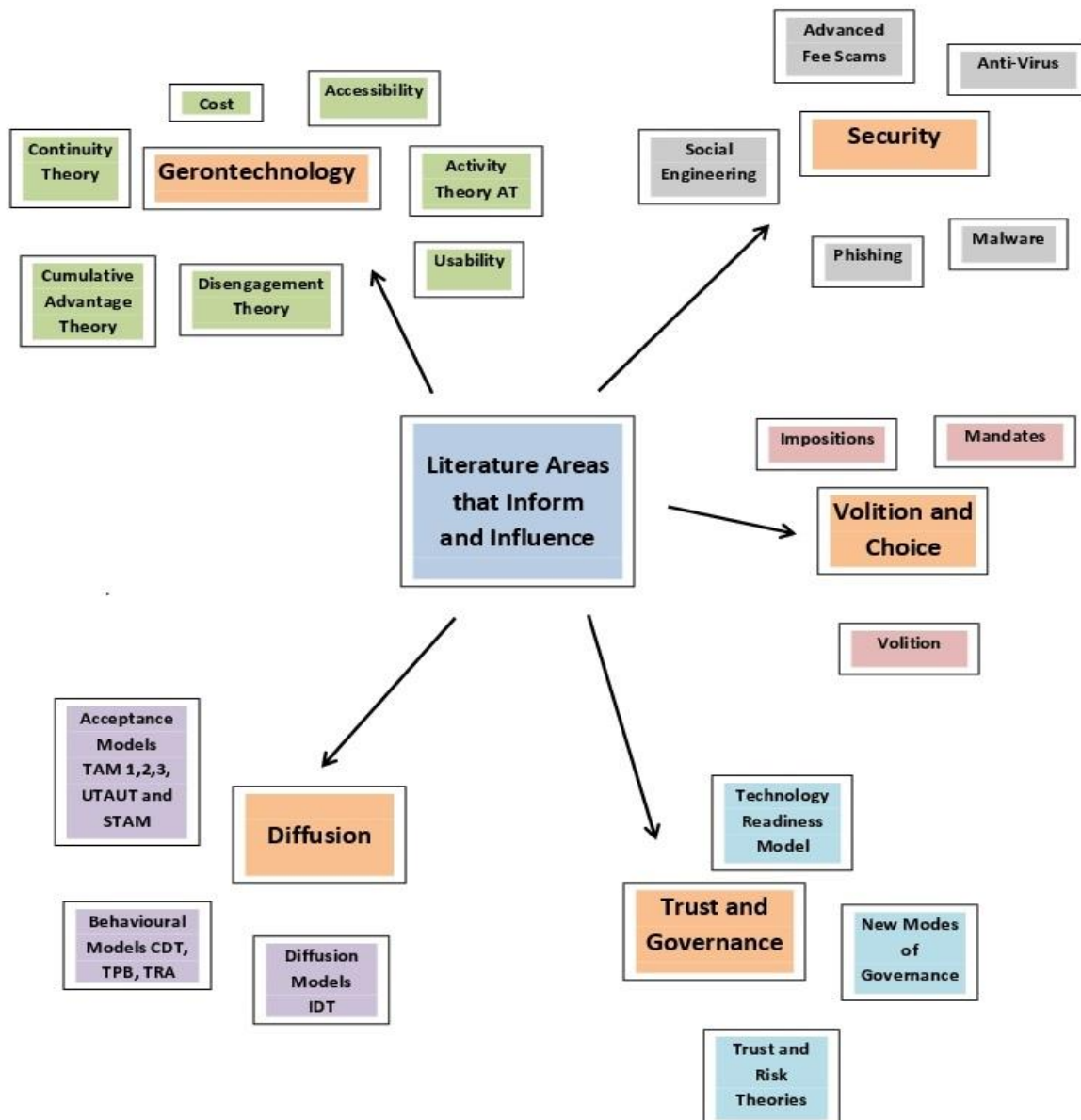
Figure 2.23. Specific areas of the literature that inform and influence the study

The literature consistently demonstrates that older people have been reluctant to embrace new ICT innovations, and specifically that there is hesitation to engage in activities of financial risk such as online and mobile internet banking. In part the hesitation is discussed as a fear of technology, yet there are also discourses that cover the fear of losing money. As a result, there are two sets of considerations that the literature supports.

The rapid speed with which some ICT innovations spread is attractive to early adopters of technology who are sufficiently fluent in the use of banking technology that they are active and optimistic in their interactions. Older people fall into the other end of the adoption spectrum, being late to adopt (if ever) and struggling with the use of banking technology. The differences are described as stark in their contrast, and older people carry stereo-typical classifications such as low ICT understanding, aging ICT equipment, low internet communication skills, and a longing to engage in online banking transactions that incorporate human contact rather than automated responses and guidance.

Older people are also reluctant in scenarios where the use of the technology is either imposed or mandated. Older people do not correlate ICT usage with trust. They are fearful of imposed scenarios and often feel obliged to use technology such as internet banking because of a sense of obligation, or as a way of maintaining the perception that they are knowledgeable about technology use.
The literature indicates that there is a need to develop relationships and cultural understanding of technologies, their vendors, and the need to socialise and synthesize ideas amongst their communities before deciding to adopt or use a banking technology.

The literature reveals that older people are targeted for cyber-crime, and that this adds to the already high-level concern of older citizens who do not wish to be taken advantage of by an online interaction. Many older people clearly voice the desire for banking in person, with face to face interactions with bank staff. Older people hold a range of view about banking safety, including that they see themselves as more vulnerable than others. Older people make the distinction between their ability to recognise deception and fraud when meeting people face to face, as opposed to placing a belief in an online system that will prevent them from having a human conversation, or of socializing ideas with

others. Older people hold a general mistrust of the Internet, and this mistrust probably carries across into the specific area of financial banking.

Older people hesitate to use online banking because there is a significant cost to using such a system. This possibly includes the need to purchase a computer, printer and paper, whilst coping with other additional needs such as the cost of training (both in time and money), and the ongoing nature of using technology. Many older people face difficulty in understanding software upgrades, new hardware, and in making informed choices about the right equipment or products to buy.

Some cite a problem with accessibility issues. A conclusion from the literature reviewed might be that there is wide-ranging difficulty with seeing and using technology. Some older people have switched to tablet computers, yet still experience difficulty with technology in the form of online forms, access to logins, and stable systems that operate in Wi-Fi mode.

The literature also indicates that older people do not trust online technology. In particular, they find that those systems that are mandatory to use, as well as those which have been imposed, are difficult to trust. Online systems are also difficult for seniors, because older people place greater trust in people than machinery. Internet banking is, for some, a difficult exercise without the two-way relationship that can be experienced in a face to face banking sense.

The literature also looks at a wide range of adoption and usage models. Whilst the technology acceptance models, the diffusion models, and all of their associated spin-offs are widely cited as indicative of usage-based trust, there is a consistent layer of writing that points to difficulties with imposed or mandated technology use, as well as the need for better online safety and security.

Each of the individual concerns that the literature raises up as barriers to trust and usage are associated with variables that reduce the expectation of technology usage and trust. These variables should not be seen as stand-alone challenges, but as part of a much larger, incomplete understanding of the need for trust by older people in the area of online banking. They are best addressed both physically and socially as required for older people to accept the social fabric of their online community and to understand the need for a culture awareness, socialisation, and integration with online internet banking.

In a more general sense, the review of the literature has revealed the way in which Information Communication Technology has been dispersed in terms of diffusion, acceptance, usage and trust. The literature suggests that usage of ICTs does not imply trust of ICTs. There are a range of evolved models of technology diffusion and acceptance, yet no singular model or theory adequately explains the association between ICT usage and ICT trust. In particular, there is a paucity of information that explains the relationship between trust and ICT usage when that usage is either mandated or imposed. In general, the literature is premised upon the assumption that ICT trust and usage is inevitable in any and all scenarios and that resistance or rejection of ICTs is characteristic of people who are either late adopters or are uninformed. The literature rarely offers an explanation that allows for people to choose or not choose to use ICT. There is the expectation that ICTs will be used and trusted.

A range of theories of technology acceptance and usage are discussed. Whilst these theories do not represent an exhaustive list they are representative of the dominant thinking regarding technology acceptance and evolution, as well as trusted acceptance. Many of the discussions are formulated around early adopters, rates of adoption, and spread of diffusion. Very little of these discussions focuses on late adopters. Almost none of the literature considers ICT from a non-adoption perspective. Technology acceptance is deemed as inevitable and rejecters of technology are rarely included in acceptance discussions.

This expectation of unavoidability extends to older citizens. The literature also indicates the significant disadvantage that older people experience in terms of likely targeting and exploitation of seniors over other members of the ICT community. Older people are easy prey for cyber criminals. They represent "low hanging fruit" in terms of likely targeting by crime and business who might seek to take advantage of the gullibility, naivety and trustfulness of people whose acceptance of ICT is predicated on perceived needs.

The TAM literature dominates the literature on technology acceptance with its two main elements of perceived ease of use (PEOU) and perceived usefulness (PU). Davis's persistent relation of how easy and unproblematic a given ICT might be by measuring PEOU forms one of the more consistently difficult elements in reconciling late adopter older citizens in terms of ICT usage and trust

(Davis et al., 1989). Together with the Theory of Reasoned Action (TRA) literature, the Technology Acceptance literature struggles to properly integrate normalised beliefs, subjective norms, and other variables where a 'false consensus' can introduce too great an influence on what is normative. The foundation of these norms is overly determined by early adopters, and there is little incorporation of perceived normative beliefs from late adopters. A similar problem falls onto PU and PEOU with the various TAM iterations.

The literature also illustrates that the concept of trust (in relation to technology acceptance) is not well articulated. Later models of TAM and UTAUT attempt to incorporate more fine-tuned variables. These include variables such as anxiety, social influence, and age, as these more accurately associate with notions of trust. The most attractive acceptance model that came from the literature review was STAM, (Seniors TAM) with its three stage model that not only looks at perceived usefulness but also aimed to describe the confirmation of usefulness. STAM is also one of the few models that allows for ICT to be rejected. Most TAM and Technology models are based on the assumption that everyone will accept ICTs and that older people who are late adopters will simply take more time. However, the models are still inadequate to properly incorporate mandated, imposed and voluntary differences when understanding the connection between technology usage and trust.

The literature on security provides a clear picture of the specific areas of vulnerability and risk that befall older people. The main areas are banking and financial interactions online, and the control and identity of people and their information in digital form. The literature on older people describes the specific targeted areas where seniors are most at risk. This allows for a clearer representation about ICT trust from a security perspective. Issues relating to money, privacy and identity are slightly easier (less esoteric) to reconcile in the minds of later adopters of technology. Older people have difficulty grasping concepts that exist only in a virtual form. Issues such as security, privacy, risk, theft, and disclosure are more closely aligned with real-world manifestations that connect with trust. It is easier for a novice ICT senior citizen to mistrust a digital system, application, or program than it is to trust an ICT environment where the need and usage, and their consequences, are not well understood. As older citizens' numbers

increase against a backdrop of ICT ubiquity, the need for better acceptance modelling for trusted use of ICTs by older people who are ICT late adopters becomes greatly amplified.

2.8.1 Defining the problem

The literature prompts the need for further inquiry into establishing the nature of trust for older people who use the Internet. It asks for inquiry about the way in which online interactions are used in mandated and imposed scenarios, yet trust is not always forthcoming from such enforced ICT usage. The literature reveals a gap in terms of the trusted usage and acceptance of technology under mandatory conditions. In particular, literature about technology choices by older people indicates higher levels of risk, potential vulnerabilities, and increased likelihood of financial and social difficulties for older people as they attempt to interact securely and safely with new technology.

By asking whether older people's trust in technology is diminished in cases where the technology or system is mandated (Hypothesis 1), a better understanding of technology usage and acceptance might be possible, enabling older people to grow and renew trusted interactions with technology. The benefits are widespread. They include financial security, health security, improved social welfare provisioning, and greater engagement with government services. Older people will interact and intermingle with all levels of social society if they are able to trust technology in an even-handed, equitable manner.

Further, by examining whether older people who are novices at ICTs are at risk through poor technology choices and a distrust in new innovations, it will be possible to understand, shape and regulate the environments in which older people make decisions based on coercion, fear, and unsubstantiated information.

By asking the question: "What affects the way older people make informed decisions about trust in ICT innovations that involve imposed or mandated online financial interactions?" this research will create a set of understandings that can be used to inform banks, governments, and policy makers with a view to providing technology that can be used and accepted by all of society (including older people).

The literature is clear in revealing that older people make unorthodox, unusual, and restricted choices about technology usage and acceptance. By understanding the nature of trust and acceptance of technology where its usage is either imposed or mandatory, research based on these literature gaps may prove helpful to reducing cyber-crime, financial stress, and social upheaval.

2.8.1.1   Summary of the problem to be investigated

The combination of uncertainties in usage, coupled with the rapid pace with which ICT technology is changing (Liao & Cheung, 2003; Grguric, 2012), creates an environment where older people commit to trusting people and systems involving ICTs that they otherwise might forego (Keat & Mohan, 2004; Morris et al., 2007). The impact of online crime acts as a multiplier of disadvantage to older people (Carlson, 2006; Mouallem, 2002). Older people are targeted more than other individuals for online activity as they represent comparatively easy prey for low-level attacks on security including phishing, social engineering, and password hacking (Chakraborty, R., Sankaranarayanan, & Upadhyaya, 2008; Cook et al., 2011a). Older people are more targeted by criminals for these types of online vulnerabilities than other age groups (Grimes, Hough, Mazur, & Signorella, 2010). Increasing numbers of financial activities require online ICT usage and trust (Charness & Boot, 2009). Thus older people may feel the need to engage in online financial activities whilst online financial providers (such as banks) who promote online technology are widening the interpersonal distance between themselves and their older customers who can exacerbate distrust (Benamati & Serva, 2007).

The literature shows that the key issues that inform this study into trust and mandation of the use of financial ICTs can be viewed through five 'lenses'. The actions of people are linked to what they perceive in terms of trust. People will act in accordance with what seems appropriate, except when they are coerced of required to follow an action for an external reason. The differences between the way some people trust ICTs and others do not are connected to issues of information, knowledge and perceptions about what can be trusted. The concepts of trust are complex and subjective. These are related to the ideas of others, and relate to previously established norms. The opinions and beliefs of older people are influenced by a variety of sources, but in particular by the human exchanges with peers and those in authority. Processes and abilities are an important 5th mens because they relate to the

capabilities of older people in learning about the relatively new area of ICT usage, and connect with the ability to be trained so as to maximise the use of ICTs within a trusted financial environment. These five lenses are discussed throughout the literature and are important considerations for this study.

Whilst older people exhibit wisdom and judgement across a wide range of life experiences, they are comparatively novice in matters of ICT usage (Blake, 1998; Byrne & Staehr, 2006; Manoim, 2011). Older people living in relative isolation from others are over-trusting of criminals. One benefit of the use of ICTs by seniors is the ability to decrease the feeling of isolation by engaging in online activities (Morrell, Mayhorn, & Echt, 2004). However, as a cohort they are said to "still carry the values of a past society, when people helped and trusted each other" (Jonson, 2003). Technology and the use of ICT by older citizens endure the stigma of pejorative sentiment towards late adopters of technology (Chesters et al., 2013; Rogers, Mayhorn, & Fisk, 2004). In this sense, perceptions are important because they will precede usage and acceptance. In many cases the perception that an ICT innovation is not trustworthy may drive the decision not to use that innovation. In situations where the acceptance of technology requires a holistic and complex understanding of the innovation and its associated usage, risks, and consequences, an older person may rely on the perceptions of their peers. Technology acceptance is most commonly modelled in terms of perceptions rather than actual usage (Venkatesh, 2000).

3   CHAPTER 3 RESEARCH APPROACH AND DESIGN

As a prelude to the discussion on methodology, it is necessary to firstly discuss the viewpoint of the researcher in the form of a guiding paradigm (Cohen, Manion, and Morrison, 2007). Such guidance steers the research in terms of the decisions and directions (Whitehead and McNiff, 2006). Guba, (1990) suggests that the determination of the research paradigm requires an understanding and characterisation of the ontology (a view of what is reality), the epistemology (a view of how something comes to be known and accepted), and then the methodology (a view of how the study should go about finding out the things it discovers and how it makes sense of them).
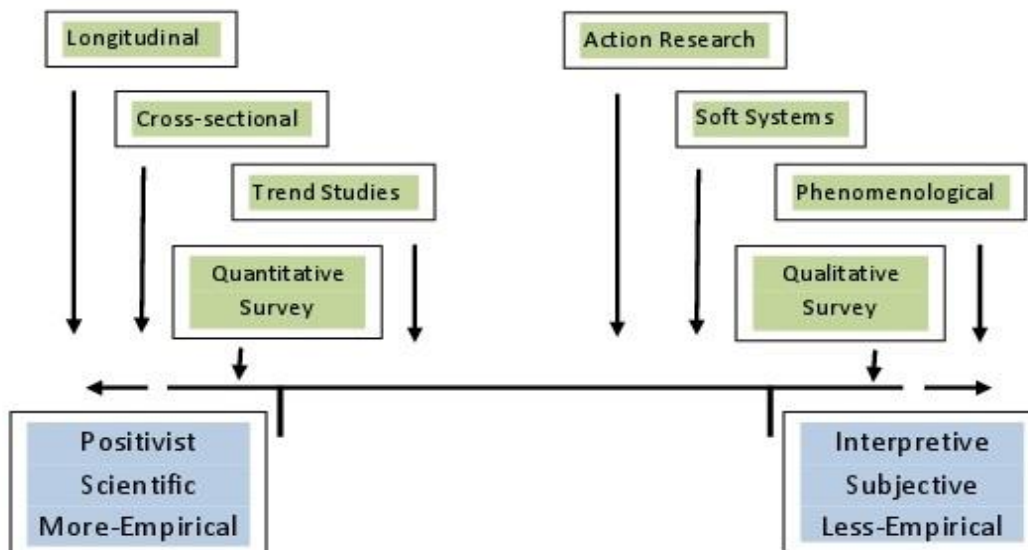
Figure 3.1   A continuum of methodological approaches to the study of trust and technology relationships

3.1   Methodology, Ontology and Epistemology

Whilst action research is the methodology of choice for this study, there is a need to describe both qualitative and quantitative research more broadly in order to understand how action research, (and not other methodologies) is the most suitable structure to steer the research forward. A research investigation is a system designed to acquire knowledge in order to advance and develop the quality of life (Cohen et al., 2008). The two overarching forms of inquiry are qualitative and quantitative research,

however the interpretive requirements of this study make the choice of a qualitative approach an important consideration.

Quantitative research centres on examining human truth and certainty by means of an organised and logical measurement. It uses the scrutiny of defined variables, and considers elements within controlled environments that are measured in terms of reliability and constancy (Somekh and Lewin, 2005). The process takes an evidence-based approach with the purpose of detailing its results and conclusions in measurable, often numerically precise and statistically ordered terms (Cohen et al., 2007).

In contrast, qualitative research aims to explore an intimate appreciation of a given phenomenon, within specific circumstances (Grbich, 1999; Pring, 2000). According to Denzin and Lincoln (1998) "qualitative researchers study things in their natural settings, attempting to make sense of, or to interpret phenomena in terms of the meanings people bring back to them". These examinations are more focussed in acquiring rich descriptions of individual perspectives. They offer functional and practical ways of understanding how social experience is shaped and assigned purpose and meaning.

Qualitative and quantitative methodologies have various differences and similarities. Cresswell's (2005) definition is instructive in understanding their aspects:

"Quantitative research is a type of educational research in which the researcher decides what to study, asks specific, narrow questions, collects numeric (numbered) data from participants, analyses these numbers using statistics, and conducts the inquiry in an unbiased, objective manner. Qualitative research is a type of educational research in which the researcher relies on the views of participants, asks broad general questions, collects data (consisting largely of words or text) from participants, describes and analyses these words for themes, and conducts the inquiry in a subjective, biased manner." (p. 39)

Qualitative and quantitative researchers take different positions in relation to social reality. They agree to accept that there is a real world, and that there is a physical reality that exists independent of our interpretations and observations. Both camps accept that this world holds a variety of properties which are of significance to scientists. From this baseline, research can be understood to take place at

different points upon a continuum (Figure 3.1) from quantitative to qualitative research (Cresswell, 2009; Cohen et al, 2007)

3.1.1 Ontology and Epistemology

This study leans towards a relativist position in terms of ontology. It is generally accepted that knowledge can be influenced by the social realities of the time, and "as such" is favoured by individual human interpretations (O'Leary, 2010). Understandings of knowledge are further swayed by values and ideals, and the societal authenticity and validity, that are created through interaction and participation (Checkland and Poulter, 2010; Bell, 2011). The epistemology is steered subjectively in this view of the world. In this study, knowledge is treated as a construct that is deduced and examined by individual interactions. The methodology that connects best with these ontological and epistemological positions is one that is interpretive, where the researcher gains insight from an analysis of perceptions within the specific setting that represents the location of research significance. Atkins and Wallace (2012) posit that interpretivist studies enable the researcher to understand the context of the specific details and to then improve the situation by means of practical and authentic interventions and involvements.

Choosing a suitable methodology for this research is a contested endeavour, since there are several variables that are indicative of a subjective, and at least partially prejudiced or preconceived set of ideas and resources. (Cresswell, 2009; Morse, 1994; Kumar, 2011). The researcher must develop research questions and must use the skills at his or her disposal that are based upon prior experiences, an understanding of what might be possible, and a belief in the capability to conduct research (Walsham, 1995).

In this research, a methodology based upon action research was favoured, because it allowed the researcher to investigate, experience, and contribute to a progression of research-based activities that formed the basis of both interpretive and informative endeavour (Hopkins, 1985; Cohen et al., 2007). The rationale that forms the basis of this methodological choice explains the framework that has been chosen. Given that the ontological and epistemological positions of the researcher are relativist and interpretive, the choice of methodology is for one that has a stronger orientation towards qualitative

research than quantitative research. The problematic challenge to examine the decision-making of older people in their trust of mandatory and imposed technologies requires a methodology that can unpack subtleties, differences, and complexities within a disordered environment (Checkland and Poulter, 2009; Dick, Passfield, and Wildman, 1995).

There are many different approaches to a study of this type, and the process of establishing an approach required the consideration of a number of different views from the literature. From the work of several authors in the field of research methods, notably Galliers (1992), Dick (1993), and O'Leary (2010), an explanation of the research approach considerations is described here (Table 3.1).

The more empirical methodologies show three types to be of significance in a study examining trust and technology relationships. Longitudinal, Cross-sectional, and Trend Studies are all well regarded methodologies but are all constrained by their inability to incorporate interpretive observations in complex and disordered situations. The importance of differing beliefs and the need to identify and examine subjective norms, makes those methods at the positivist side of the methodology continuum less appealing to the needs of this type of study.

The less empirical methodologies are best represented to examine trust and technology relationships through Action Research, Soft Systems, or Phenomenological studies. These methodologies are more interpretive than empirical, although phenomenological studies can include empirical observations if they suit other perception-based observations. Phenomenology is the least suitable for an examination of trust-relationships because it relies on perceptions of empathy and includes intersubjective elements, which can be misleading and can rely heavily upon the bias of the individual researcher or research team. Having eliminated Phenomenology as a possible methodology, the two preferred remaining methodologies are Action Research and Soft Systems Methodology. They are preferred because they both allow for a divergent set of views to be examined, using complex situations, where there is a need for a close examination of a rich rather than a large data set.

Table 3.1 A Description of Methodologies suited to a study of trust and technology relationships.

Method	Approach	Limitations
Longitudinal	Data collected over a long period of time involving repeated observations of the same variables. They observe the state of the world without attempting to change or manipulate it. It aims to achieve correlational findings.	It is argued that longitudinal studies have less power to detect causal relationships than other methods.
Cross Sectional	Cross-sectional studies use cross-sectional regression in order to understand the presence, and the scale, of causal effects. They typically measure the effect of one or more independent variables on a dependent variable at a given point in time. They can describe odds ratios, prevalent, and relative risks.	Where multiple factors are in play, cross-sectional studies are often unable to identify which variable is the cause and which is the effect.
Trend Studies	Trend studies are aimed at collecting data in order to identify a trend, pattern or inclination towards one element over another. It is highly used where the statistical measurement of quantitative data allows for a discovery. It uses regression analysis to identify the relationships between dependent and independent variables	When measuring small effects or inquiring into the identification of causality, trend studies can give misleading results.
Action Research	Describes rich data from within an environment. Includes intervention and reflection components. Uses a real-world setting and iterative cycles to include action, reflection, and participation	Interpretations remain criticised for subjectivity. Lack of control of variables. Findings may not accurately translate on broader terms.
Soft Systems	Uses systems thinking to identify complex problems – especially where there are divergent views about what the problem(s) may be. It can be useful in complex problems.	Soft systems are limited because they require participants to adapt to an overall approach. In instances where the scope is narrowed at an early stage, they can give misleading results. For the richest results – SSM requires the imposition of a specific structure. In some instances, describes as "the cure is worse than the cause".
Phenomenology	Aims to obtain interpretive and descriptive data to explain connections between beliefs, norms, preconceptions, and the social situations in which they occur. It relies heavily upon judgements, perceptions and emotions. The process sometimes overlooks traditional data in preference on relying on the value of reflections and the conscious experience	The interpretive nature of this method is criticised for researcher bias and the inability to exclude other explanations. By overlooking some traditional data in favour of perceptions, phenomenology receives criticism for throwing aside important considerations rather than attempting to combine various different elements that may be found in the process of discovery.

3.1.2 Action Research or Soft System Methodology?

Of the methodologies under consideration the two that were suggested by the research literature to have the best fit were Action Research (AR) and Soft Systems Methodology (SSM). This section explains why AR was used in preference to SSM. Both approaches provide an ordered way of engaging in observed problematical societal conditions (Checkland and Poulter, 2010; Wilson and Van Haperen, 2015). Both have an ordered system of thinking about such situations so that action can be undertaken

in order to bring about change and improvement (Checkland and Poulter, 2010; Wilson and Van Haperen, 2015). Equally AR and SSM recognise the complexity of social situations, and both acknowledge the existence of different views with different people and within different places. They both operate from an assumption of many different world views, and they both take into consideration the added challenge that for many people such views can be fixed from their own viewpoint. Both AR and SSM understand the value of purposeful endeavour, so as to bring about change through action based on a sense of purpose. The criticism that is well documented in the literature about Soft Systems is in the application of an "all in" agreement by participants as to the systems solution (Wilson and Van Haperen, 2015). This can be problematic in complex situations, and is an unrealistic expectation given the rich and varied nature of older people and their interactions with technology (Ivanov, 1991; Checkland and Poulter, 2010). Furthermore, this study specifically examines the problematic nature of mandatory or imposed technology use by older people. Thus the notion of a participatory acceptance of a systems solution makes Soft System Methodology an unlikely candidate for the best approach to this study (Ivanov, 1991; Wilson and Van Haperen, 2015).

By adopting action research as a method of inquiry the researcher is using a method that is well suited to professional and personal dimensions where there are issues of choice (Noffke, 1997; Atkins and Wallace, 2012). It allows for an examination of existing practices that might be bound by regulatory and social elements that can be problematic in terms of the rapid change that often impacts upon access and social justice matters. Cohen et al. (2008) suggest that action research is an appropriate method where there is a need to adopt a novel system for understanding different new ways of learning, deciding and professional development. The methodology has a wider inclusion of factors such as hierarchy, experience, and other delineations that are sometimes masked in other formats (Grundy, 1995; McNiff, 2013).

3.1.3   Determining the appropriate approach

Action Research was determined to be an applicable approach to explore the topic, after the completion of an analysis of possible methodologies. Action research is a broad church of inquiry that allows an open-minded approach to what is the representative data, and which elements represent

compelling evidence (Cohen, Manion and Morrison, 2007). It permits a wide scope of evidence that includes accumulating and analysing findings, responses and reflections about what is taking place (Gergen, 1999; Holstein and Gubrium, 2008).

Action research is considered to be a potent instrument for the improvement of groups who are disadvantaged in areas of learning, training, access, prejudice, socialisation and quality of life (Lewin, 1946). It is particularly useful in areas where there is a social problem where there is an existing awareness of a problem, and an accepted need to change something in order to improve the consequences of that problem (Kemmis and McTaggart, 1988; McNiff, 2013). Action research allows for the development of a rich theory that incorporates formal research, knowledge from practitioners and users, and in-depth reflection upon those elements (Richardson, 1994). The emphasis of action research is upon advancing the quality of the action within the frame of inquiry (Elliott, 1991).

By adopting action research as a method of inquiry the researcher is using a method that is well suited to professional and personal dimensions where there are issues of choice (Noffke, 1997; Atkins and Wallace, 2012). It allows for an examination of existing practices that might be bound by regulatory and social elements that can be problematic in terms of the rapid change that often impacts upon access and social justice matters. Cohen et al. (2008) suggest that action research is an appropriate method where there is a need to adopt a novel system for understanding different new ways of learning, deciding and professional development. The methodology has a wider inclusion of factors such as hierarchy, experience, and other delineations that are sometimes masked in other formats (Grundy, 1995; McNiff, 2013).

3.1.4   Background to the methodology

Research of this kind (Action Research) can be embarked upon both collaboratively and through participative action (Koshy, 2009). The research is situation-based and context specific (Atkins and Wallace, 2012). The research allows for the development of reflections based on interpretations made by the participants (Zuber-Skerritt, 1996). This results in knowledge that can be applied to solve a problem, and to improve an existing set of practices that call for change (McNiff, 2013).

Within the action research collective, the *emancipatory* strain of action research is strongly coupled with many of the professional objectives and products of this study. Grundy (1987) suggests that *emancipatory* action research can assist participants to better understand structural and interpersonal constraints that in many cases prevent them from interacting freely and with fewer limitations. These limitations are often barriers to the development of technology learning when practices are enacted without a more balanced sense of autonomy, social justice, and self-determination (Grundy, 1987; Giroux, 1986). The emancipatory style of action research centres on constructing a system of meaning in order to guide a process that collects information from a variety of different sources, makes sense of the data, and adopts a purpose of setting free the participants by means of praxis-based solutions (see Table 3.2) (Kincheloe, 2003).

Table 3.2 Emancipatory Action Research (Kincheloe, 2003)

	Steps for Emancipatory Action Research
1.	Constructing a system of meaning
2.	Understanding dominant research methods and their effects
3.	Selecting what to study
4.	Acquiring a variety of research strategies
5.	Making sense of information collected
6.	Gaining awareness of the tacit theories and assumptions which guide practice
7.	Viewing teaching as an emancipatory, praxis-based act.

The process of creating praxis-based solutions is galvanised by the addition of reflection (Cohen et al., 2007). Reflections allow the researcher to make sense of a variety of data sources and to incorporate elements such as group cultures, language and discourse, social structures, and behaviours, actions, and practices (Kemmis and Taggart, 1992, McNiff, 2002). They aim to give groups the ability to take control over their lives by promoting appropriate change that is based upon research strategies that challenge and question given value systems (Habermas, 1987; Giroux, 1986). The literature on older people's acceptance and trusted use of technology suggests that mandatory and imposed practices withdraw many elements of choice (Charness and Boot, 2009, McMillan, Avery, and Macias, 2008).

Thus in a general ideological sense the inborn endeavour to develop emancipation is aligned with Lewin's (1946) view of a critical praxis that evolved cooperation and reduced exploitation.

Since Action research has a broadened set of inclusions, some scholars tend to describe what the process does not involve rather than stating what it is. Kemmis and McTaggart (1992) explain that their view of action research thinking and reflection is not analogous with the normal everyday thinking that everyone does. Instead it is a systematic process that collects evidence so that reflections are exacting and meticulous in their detail. They state that action research is more than simply problem solving, but rather it is a problem that also identifies and poses problems in addition to unravelling them. Furthermore, there is greater emphasis on understanding within contexts, and prescribing alterations that incorporate changes to values and beliefs, and transformations of theories and practices (Noffke and Zeichner, 1987).

This chapter has so far described the methodological background that has been used in this research. It outlines the processes that were arranged for a qualitative approach of this kind. There is an explanation of the interpretive research methods that have been chosen, which forms the rationalization for the manner in which the data and evidence have been accumulated.

This research draws its methodological characteristics from what Winter (1996) describes as the six key principles of action research (Table 3.3). These principles are woven into the approach taken for this study.

Table 3.3 Principles of Action Research (Winter, 1996)

Principle	Description
Reflexive Critique	The practice of becoming conscious of our own perceived predispositions
Dialectical Critique	Observing and perceiving the associations and interactions between the components that comprise different phenomena in a given context
Collaboration	The inclusion of all views and ideas as a standard for understanding a given situation
Risking Disturbance	Subjecting those processes and ideas that are taken for granted and offering them for evaluation and analysis
Creating Plural Structures	Developing various explanations and analyses, instead of a single commanding version
Theory and Practice Internalised	Seeing theory and practice as two mutually supporting yet corresponding segments of the transformational process

The process is inclusive, allowing the researcher to be genuinely inquisitive as part of the thorough analysis and reflection of information. Action research involves comparing a range of conditions and effects by means of a spiral of steps, incorporating reflection over iterations so as to compose a circle of planning, action and fact-finding that is derived from an evaluation and contrast of the elements examined (Atkins and Wallace, 2012). Action research has as a central purpose the objective of solving a specific problem and providing a framework or a set of guidelines that assist in the pursuit of better practice (Denscombe, 2010). It can focus upon actions taken that are set against a reflective understanding of those actions (Reason and Bradbury, 2007; Atkins and Wallace, 2012). In this sense it is an appropriate method for improving the actions of certain groups and cohorts that could provide the guidelines for large-scale change (McNiff and Whitehead, 2005). It is described as a research style that aims to bridge the gap between research and practice by means of training and education (James, 1988; Stenhouse, 1979; Somekh, 1993).

Much of the literature on action research is heavily tailored towards a teaching and learning setting (Kemmis and McTaggart, 1992). The word classroom is often used to discuss the virtual environment that surrounds the reflective aspects of the research development (Grundy, 1995). Such descriptors strongly resonate with the idea that older people are looking to resolve their technology-based trust and choice issues by means of an educational vessel that allows for existing life experiences to integrate with technology-driven changes (Crane, 2014). Action research is therefore an appropriate framework to deal with specific concerns that are acknowledged by local people, to amend customs, and to utilize those changes to decipher problems (Goff, 2007; Crane, 2006; Reason and Bradbury, 2007).

3.2   The rationale for selecting Action Research as an appropriate methodology

This chapter has explained a process by which research methodologies were initially considered because of their appearance in the literature. Factors included their previous use in other studies that had connections with trust and technology usage, and their suitability to studies relating to technology change and cultural and behavioural variables. From this initial process six methodologies have been

discussed, allowing for an understanding of the comparative features of methodologies from both the quantitative and the qualitative ends of the research methodology spectrum.

The process was further distilled and in so doing it identified two methodologies: Action Research and Soft Systems as potential approaches to the research. Finally, Action Research was chosen because of its suitability to the discovery of a rich set of data, and an iterative and reflective set of cyclical processes that incorporate real world situations, reflective and participative contributions, and a high likelihood of a set of outcomes that are practical, applied, and relevant. Action Research has been described as not one methodology, but more like an assemblage of methodologies that sets about to invoke transformation, accomplishment, understanding and knowledge in a single package of discovery (Dick, 1999; Checkland and Poulter, 2010).

3.3 Research method

Choosing to use a design method which incorporates an interpretive style meant that the data obtained from interviews would allow for an iterative and reflective engagement with the data collection and analysis. By using a qualitative design approach based on action research, it is possible to gain an understanding of the processes and decision-making of older people who establish or reject trust in ICTs. This research serves to reveal conjectural and pragmatic perspectives for establishing ICT-trust under mandatory or imposed conditions.

This section explains the use of cyclical research whereby each cycle is based upon planning, action and critical review. This cyclical approach takes time iteratively to observe, reflect, and analyse each undertaken step before proceeding to the next step (see Figure 3.2). By using additional observation and reflection processes it is possible to realize and to bring to the surface any discrepancy and differences occur, and using those inconsistencies to shape and inform the research (Wadsworth, 2006). In this way, new ideas that are recognised can be further explored in each new iteration, as well as with each new action research cycle. Multiple iterations including observations, reflections, and analysis are performed in each of the three action research cycles (see Figure 3.2). The design method incorporated a systematic literature review, a set of semi-structured interview questions, a system of data analysis that incorporated both hypothesis-driven analysis and content-driven analysis, and a case-study comparison. A description of the method is given here.

The literature review focused on five main areas of discovery. They were cyber security, volition and choice, gerontechnology, technology acceptance, and trust and governance. From the review of the different literatures a set of interview questions, as well a set of hypothetical examples were created.

3.3.1 Sample strategy

Participants were selected from a purposive target sample of clubs and associations who represented the interests of older people. The target group were all over the age of 60, and no longer full-time employed. Four associations each announced that there was a request for participants, and

people came forward citing an interest in involvement. These initial volunteers were used as informants within the associations to identify others who would qualify for the research. Participants were asked to volunteer if they thought of themselves as novice users of ICT. By using this snowballing technique from four associations, three hundred and twenty (320) names were listed and the names were randomised using the RAND random number function built into Microsoft Excel. Systematic sampling was used to select participants from the list with every tenth random number providing a participant for the sample. A total of thirty-two participants were drawn for interviewing. The sample size of 32 made allowances for redundancy, with the final number of participants being reduced to 28 after four respondents revealed high-level knowledge and understanding of ICTs.

3.3.2   Interviews

A total of 45 interview questions were prepared, as well as 12 specialist scenario propositions to consider. This was broken into 4 sections of interview questions and 1 section focusing on specialist scenario propositions. The interview questions consisted of 9 qualifying questions to identify respondents as older people who did not have professional-level ICT skills and who had not undertaken high-level specialised training in the area of online banking or financial management. These were followed by 22 questions focusing on ICT usage, with a specific emphasis on communications, financial circumstances, and where security exploits might occur. The third section of interview questions consisted of 5 questions where respondents were asked to describe trusted ICT interactions, and were expected to respond to questions that informed the way in which they attempted to reconcile their ideas about technology trust. The fourth section asked about conditions where a decision to trust occurred. Respondents were asked to explain their thinking when deciding to either trust or to reject ICT usage. The fifth section did not ask specific interview questions, but instead put forward a range of hypothetical scenarios where trust-based decisions might be involved. The respondents were expected to identify and evaluate propositions along the lines of trust, usage, risk, and change.

.
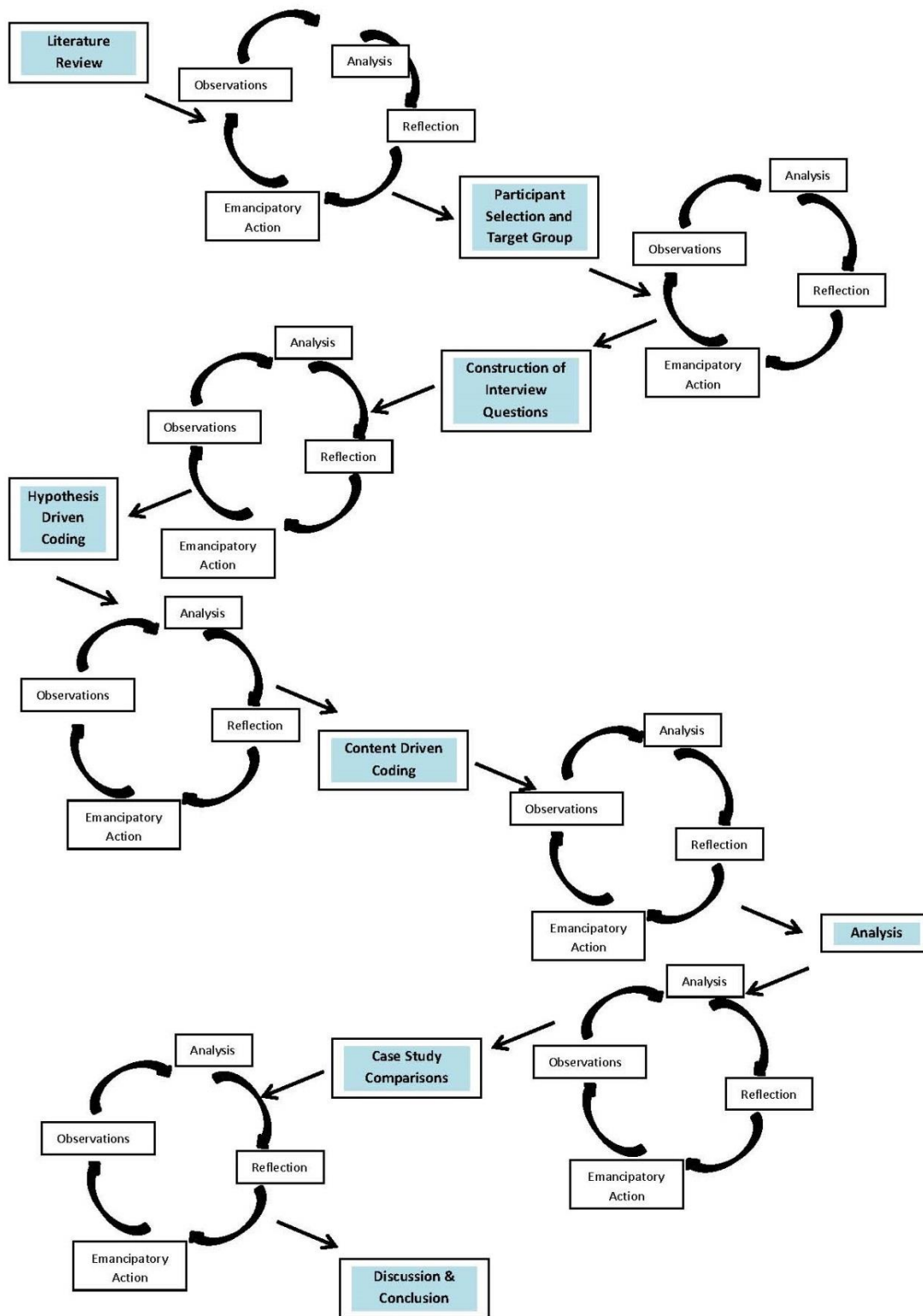
Figure 3.2 Design for the Study

The respondents were to be asked to answer questions built upon hypothetical situations, each one depicting an element of either imposed or mandatory ICT interaction. There were twelve hypothetical scenarios requiring response and explanations. The data from the interview questions, as well as the data from the hypothetical questions would then be transcribed, and then coded. The coding was a two stage multi-iterative process. It included both confirmatory (hypothesis-driven) coding as well as exploratory (content-driven coding). These interview data results would be analysed after coding so that a full analysis could be made (Figure 3.2).

This analysis is referred to by Guest, Namey, and Mitchell (2013) as the *Confirmatory* (or hypothesis-driven) form of analysis. It is characterised by an inductive orientation where many specific codes and categories are predetermined prior to the analysis. (Table 3.4)

Table 3.4 Confirmatory (hypothesis-driven) approach to data analysis

Confirmatory (hypothesis-driven)
• For example, hypothesizes, "X attributes will be found more often in data from source Y than from source Z".
• Operates from a deductive orientation
• Specific codes, with analytic categories some of which have been predetermined prior to analysis
• Coding has some predetermined structure
• Codes are generated from hypotheses or borrowed from existing sources
• Previous elements generated from probability sampling

A second form of analysis then follows the first. This analysis is far more reliant upon the content of the transcripts than it was upon previously determined structures and themes. At this stage the coding is done in two ways. The researcher re-codes the main themes using content rather than hypothesis-driven thinking. At the same time, the transcripts are run through the software program NVivo 8 as part of a secondary attempt to employ sense making through common themes and styles (QSR International, 2013).

Thus, the second level of coding allows for richer, and more finely detailed appraisal of the results. It still takes into account the previously undertaken confirmatory coding analysis, but goes

beyond these structures to form new segmentations in what Guest et al., (2013) refer to as *Exploratory* (or content-driven) analysis (Table 3.5)

Table 3.5 Exploratory (content-driven) approach to data analysis

Exploratory (content-driven)
• For example, asks, "What attributes are observed/identified in sample X?".
• Operates from an inductive orientation
• Specific codes and analytic segments are NOT predetermined.
• Coding is open-ended
• Codes are derived from the data.
• Can use either non-probability or probability sampling

From the analysis of the interviews and scenario considerations the data would go through coding and analysing processes to allow for an exploration that included iterations of reflection, observation, and scrutiny. The process is intended to provide multiple iterations of the review and analysis of data to obtain high-level information from a rich data set.

In order to support the analysis in order to make conclusions and inferences, the design includes some validation of the analysis of the data against a set of case studies. This was included in the design so as to compare to interpretations and conclusions against known examples to see if there was commonality that would reveal a stronger acceptance approval of the data results and analyses.

3.4 Limitations of Action Research and how they are addressed

All research has limitations (Cohen et al, 2008). Action Research is limited insomuch as whilst it recognises the existence of multiple world views, it also acknowledges that different views change "over time" (Checkland and Poulter, 2010). A static set of world views does not suit Action Research, since it opposes the idea of social problems that are fixed to a point in time, and prefers to discover findings by means of qualitative data rather than quantitative numbers. Therefore, the research findings may hold less currency "over time". By retaining comparison with known trust constructs, the value of the findings will hold value "over time", irrespective of the changing views towards technology and ICT usage.

Like any non-empirical study, Action Research is limited by the subjective interpretations of the researcher (Wadsworth, 2006). Since there are usually multiple variables, and a range of individual differences, the possibility of subjective bias cannot be excluded from this study. In terms of addressing the subjective nature of the approach, the researcher accepts the action research methodology for what it is, an approach that is inherently designed and structured in order to elicit a subjective perspective that can deliver new understanding in the field of endeavour (Reason and Bradbury, 2007; Zuber-Skerritt and Fletcher, 2007).

Notwithstanding the possibility of bias through subjectivity, strong rigour can be reached through two key elements in the research methodology. In defence of a rigorous AR-based methodology for this research the design includes double loop learning (Argyris, 1991, Zuber-Skerritt and Fletcher, 2007) and an observational and reflexive system of examining and analysing research data (Johns and Burnie, 2013). As earlier described, (see Table 3.2) the use of emancipatory research is designed to allow situations where the existing thinking about the problem should also be critically evaluated. This process, as described in action research (Cohen et al, 2008), uses reflexivity to include both the raw data from the research along with a number of reflections upon the established and existing view of things (Figure 3.3).
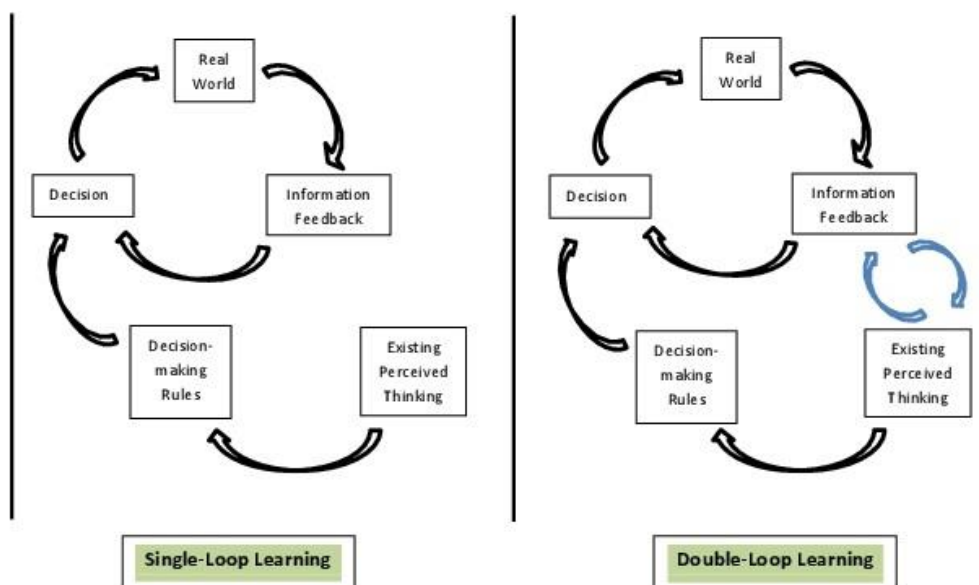
Figure 3.3 Double Loop Learning and the Reflexive Feedback Loop (Argyris, 1991)

138

In this research, reflexivity, and the integration of critical reflections, provides an important cornerstone for an epistemological understanding that evaluates not just the participants of the interviews, but the underlying existing views about technology usage and acceptance. Thus, without the combination of both interview data from active participants, and the ability to challenge and contest an existing expectation placed upon them, an important dimension to the critical analysis of this research proposition can be under-represented (Fisher and Phelps, 2006; Zuber-Skerritt and Fletcher, 2007).

The next chapter discusses an extension to understanding issues of trust and technology. It considers issues about usage, choice, and capability in relation to how trust and technology are affected.

4   CHAPTER 4 TECHNOLOGY AND TRUST-DRIVEN RELATIONSHIPS

The purpose of this chapter is to build on the information drawn from the intial literature review to better understand concepts that will more directly inform the hypothesis in regards to ICT trust, ICT usage, choice, and capability. To do this it looks at what the literature shows to be strong trust-driven relationships.

The literature review in Chapter 2 looked broadly across a range of areas of influence about technology and trusted usage. With specific reference to the research question that asks what affects the way older people make informed decisions about their trust in new ICTs that involve imposed or mandated online financial transactions, the literature identified two main areas. Firstly it showed that older people generally made poor decisions in terms of risk, security, and practices. Secondly it identified gaps and uncertainties about how older people choose (or have difficulty in choosing) how and why they might trust new ICTs.

By examining what reduces trust, and looking more closely at some assumptions that are associated with trust, the emergent gap in the literature is that requires attention is to show that usage does not imply trust. For example, a great deal of the technology acceptance literature is heavily premised on the idea that continued usage "over time" equates to trusted usage. However, different factors other than usage, affect the trusted acceptance to choose and to use ICT technologies. Older people's ICT usage changes when the ability to choose an ICT is removed, reduced, or influenced. The literature identified many uncertainties in relation to cyber vulnerabilities and the differences between novice ICT users and experienced users. ICT trust and usage choices can be characterised as reactions to perceived risks.

The relationship between technology and its trusted usage underpins this research. The initial review of literature suggests that trusted acceptance of technology comes from usage. However several different ideas emerged alongside the notion that usage creates trust. The first was that older people were disproportionately reluctant to use and accept technology. The second was that despite a series of progressively developed approaches to technology usage, mandatory and imposed interactions failed to gain trusted acceptance. A third element, although not as prominent as the first two, was that technology

practices involving the secure use of systems for financial transactions and daily living, were problematic in terms of online security, ICT capability, and accessibility.

4.1 Misconstructions, and Missing Constructs

The literature was focused upon five main areas of inquiry, and specifically concentrated on behaviours, case studies, incidents, and models that would demonstrate and explain how older people make decisions relating to the secure trusts engagement with technology and ICTs (Figure 4.1). A consistent, recurring exclusion in the literature came from the repeated assumption that new technology usage was better, rather than that many new technology systems were different. Thus in a general sense, it became clearer as to what factors informed the study, and what areas remained fixed on the idea that usage equated as trusted acceptance (Figure 4.1). The studies showed an absence of volition, rejection and imposed considerations.
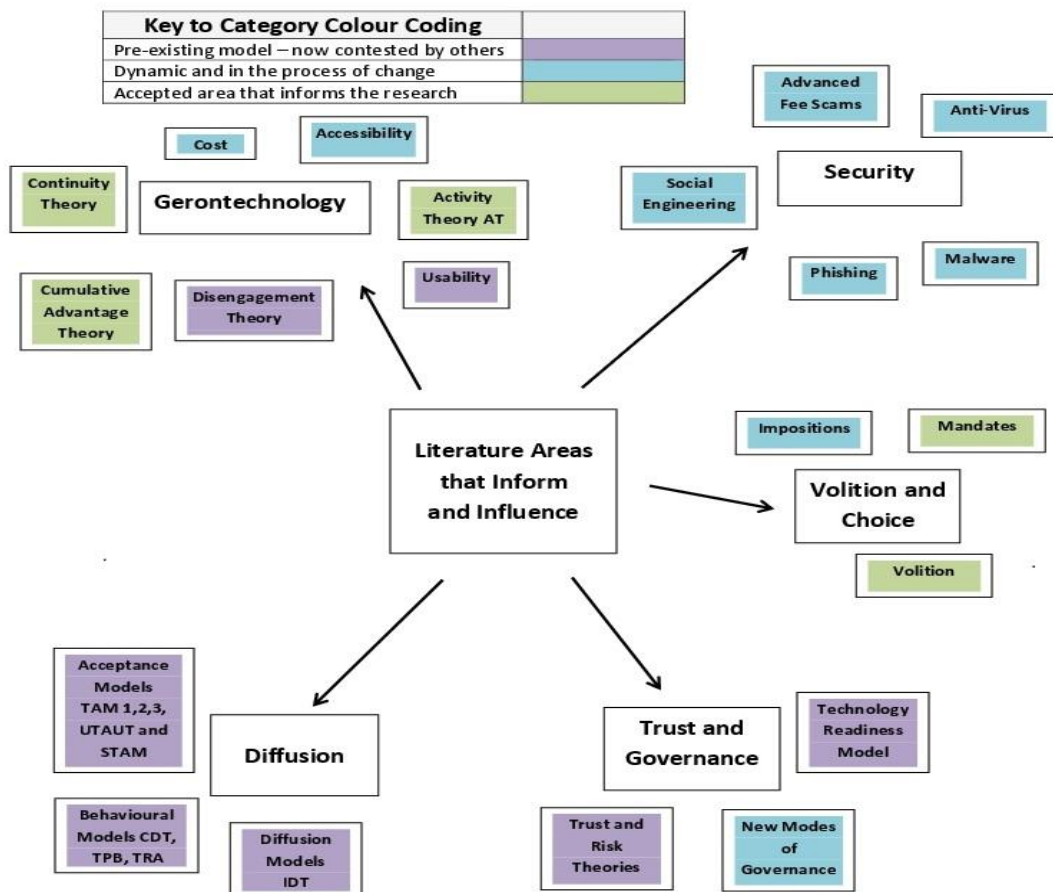
Figure 4.1 The literature areas showing areas of contest, change, and agreement.

Whilst all five of the areas of the literature revealed information about the general use and acceptance of technologies, very little was revealed about trust where the usage was forcibly imposed required. Where the usage came from voluntary action, the connection to acceptance is stronger than when the usage was undertaken as an imposed or mandated action. Perceived risks, hesitations, security concerns, age-related criteria, and the governance of older people's technology choices were all identified as emergent factors. The review concluded that trusted acceptance was influenced by perceptions of a variety of challenges. These included financial risk, technical incapacity, apprehension towards non-human systems, cost of computing, criminal superiority, inaccessibility, enforced change, a lack of communication, targeted exploitation, identity manipulation, information misuse, privacy breaches, and many smaller trust uncertainties. The literature pointed to many reflections of a previous era with a significantly more human set of interactions, with less complex systems, less sophisticated criminal activity, and a far smaller reliance on ICT-based interactions.

The choice to use technology is identified as being connected with the trusted acceptance of that technology. Some technology usages are not voluntary. Under normal conditions, acts of volition are characterized by conscious decisions that are purposeful acts of commitment towards a particular intention (Kuhl & Fuhrmann, 1998; Deimann & Bastiaens, 2010). There is a need to distinguish between voluntary ICT usage and mandatory usage, or imposed usage because the literature on older people establishes that there is a problem between their need for trust and their need to interact with ICTs. One significant area of trusted and secure ICT usage occurs in connection with financial interactions for the purpose of banking. Understanding the interplay between usage and trusted acceptance of ICTs in banking helps to inform the critical association between imposed and mandated interactions and trust for older people.

4.2   Refining Trust and ICT variations: a focus on criticality

The connection between usage of ICTs and trust is born out strongly in cases where older people interact with ICTs for financial purposes. Older people show greater concern over finances than younger aged cohorts because once retired they have little opportunity to rebuild or recover from severe financial

loss. The literature revealed eight major areas where trusted acceptance of ICT usage was likely to be negatively affected by mandatory and imposed conditions. Table 4.1 summarizes the eight major areas where mandatory and imposed conditions might reduce the trusted acceptance of ICTs.

Table 4.1 Issues affecting trusted acceptance of ICTs

<table>
<tr><td colspan="3">Issues affecting Trusted acceptance of ICTs</td></tr>
<tr>
<td>1</td>
<td>Issues of Diffusion</td>
<td>(a) ICT emphasis rapid diffusion of ideas (1st to Market)
(b) New ideas rolled out that exclude Non-ICT options
(c) Seen as inevitable that users will choose an ICT solution over a non-ICT solution</td>
</tr>
<tr>
<td>2</td>
<td>Issues where Choice is removed</td>
<td>(a) Enforced and imposed ICT systems force usage before trust is established
(b) User demotivation to try new technologies where the usage is enforced.
(c) Reduced / Partial trust in systems that are mandatory
(d) Cultural differences between digital immigrants (older people) and digital natives reduce expectations of trust.
(e) Reduced motivation to use systems perceived as complex.
(f) Reluctance towards digital storage of information (prefer paper systems)
(g) Reluctance towards cloud storage (prefer physical / tangible ownership and access
(h) Issues with reliability and responsibility where face to face human contact is removed as an option</td>
</tr>
<tr>
<td>3</td>
<td>Issues where usage does not equate to trust</td>
<td>(a) Assumption that usage "over time" guarantees trust not accepted where usage is mandatory
(b) Prevailing norm with older people that tried and tested non-digital systems are less dangerous.
(c) Choice of system regarded as an important transparency to guarantee trust

(c) Mandatory usage cannot claim to be trusted without sufficient legitimate power or authority.
(d) Mandatory systems need to demonstrate an acceptance process of choice, socialization, and wider community discussion.
(e) Forced change from one ICT system to another must show transparent due diligence to ensure trusted acceptance</td>
</tr>
<tr>
<td>4</td>
<td>Issues of transition to ICTs from non-ICT usages</td>
<td>(a) Perceived as difficult by older people who don't see the need to change when non-ICT systems are working.
(b) Measureable difficulties by older people in terms of complexities, capabilities (e.g. Physiological age-related challenges)</td>
</tr>
<tr>
<td>5</td>
<td>Issues of forced transition from one ICT to another</td>
<td>(a) Older people socially conditioned to expect longevity in systems and in hardware components. Reluctant and non-trusting towards systems that constantly need to change and update (e.g. retention of OS such as Windows XP)
(b) Older people associate constant updates and upgrades are signs of immaturity in a system.</td>
</tr>
<tr>
<td>6</td>
<td>Imposed systems and Diminished Trust</td>
<td>(a) Incentives for early or repeat use, or to coerce a change of system can raise usage levels whilst reducing trusted acceptance.
(b) Govt-imposed ICT usage in developing communities diminishes trust and seen as an attempt to soften the impact of unfair or unjust ICT obligations.
(c) Diminished trusts occurs when increased complexity in ICT usage occurs – this reduces perceptions of reliability and trusted acceptance.</td>
</tr>
<tr>
<td>7</td>
<td>Human Interactions versus Automation and ICTs</td>
<td>(a) HI and HCI seen by older people as misaligned / incompatible. Those with little ICT training or experience equate safety and security with the manual processing of things.
(b) Fear of automated and unrecoverable financial losses using ICTs instead of humans (e.g. Bank Tellers) - Criticality of finances drives diminished trust in ICTs
(c) 24hr banking seen by solder people as risky rather than convenient. Inability to call a person if an ICT-related financial problem arises.
(d) Greater confidence in self-assessment of Human banking capabilities over ICT banking systems</td>
</tr>
<tr>
<td>8</td>
<td>Cost Issues</td>
<td>(a) Many ICT systems / computers / printers / tablets seen as too expensive to purchase by older users.
(b) Accessibility issues – poor choices – lack of ICT hardware and product knowledge.
(c) Lack of personal contact post-purchase – associated with lack of trust in hardware/software
(d) Digital systems do not allow users to "buy" privacy – lack of product knowledge –once lost, private information in digital form is unrecoverable.
(e) Additional and Repeated costs for ICT security updates when existing physical security seen as reliable and usable without significant update</td>
</tr>
</table>

In cases where technology is used to access and transact financial assets any limitations on choice of hardware, software or provider greatly reduce the trusted acceptance of that hardware, software, or provider. Critical interactions (such as financial banking) are perceived by older people as

important and "as such" generate greater resolve in terms of their trusted usage and trusted acceptance. Whenever access to choices or options is reduced or taken away because of mandatory ICT usage practices, the trusted acceptance of any new ICT system is also reduced.

4.3   Reflections on trust and mandated, imposed and freely chosen technology

If the trust relationship can be diluted by a mandate for usage, then it is more likely that the trusted security of an innovation is weakened when the usage is mandated (Singh and Morley, 2009). Figure 4.2 provides a visual example of this relationship. Note that this simplified diagram assumes a situation that is *ceteris paribus*, that is that all other parameters are equal. Thus it does not take into account a situation where a person becomes more aware of a security issue and adapts.

Technology, Trust and Security
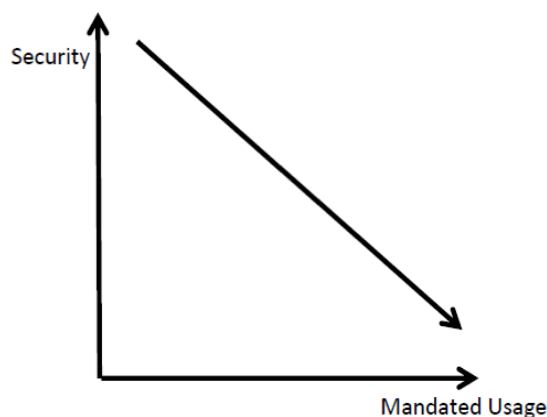
As Usage becomes more mandatory, trust in the enforced technology decreases

Figure 4.2 The inverse relationship between Security and Mandated Usage.

The security may be diluted under imposed conditions as well.   For example security is perceived as under threat where the usage is imposed. Security and Trust are jointly diluted as interactions with ICTs move from an imposed to a mandated state (See Figure 4.2).   In many instance security deliberately imposes conditions on users so as to protect the objects being used. For example, a banking app may force a user to submit to multi-factor authentication in order to establish that a user

is a human and not a scripted botnet. Older people may interpret this additional security authentication as a threat to the system, and will often trigger a response to not use the ICT-based system, but instead to revert to human operators such as banking tellers. These reversions require the ability to choose between one system and another. Thus when security is threatened, and choices are limited, trust is reduced.

Technology, Trust and Security

As Usage becomes more mandatory, trust in the enforced technology decreases
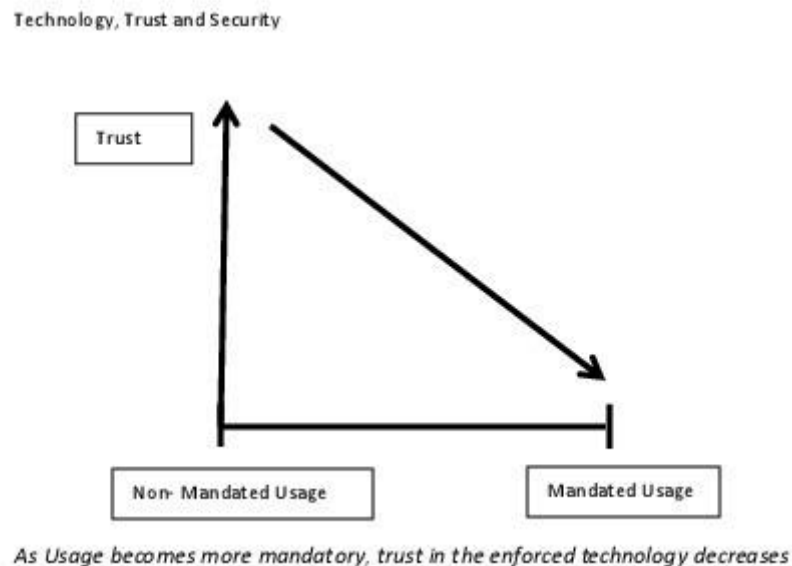
Figure 4.3 The inverse relationship between trust and mandated usage.

This can be explained in several examples.

Where the usage has been mandated by an external authority, then the user may expect that consequences arising out of such trust lie with that authority and not the user (Figure 4.3). Hence the user may not rely on their own set of precautions because they would expect an authority to provide broad systems safeguards. Passwords need not be changed or kept secure where such usage is under mandate. Patches need not be installed, or might be installed in a less than timely manner. The motivation to comply with acute and careful vigilance shifts to a lower level of attention. This instead changes to compliance with the least amount of effort.

Such a shift in effort might not just extend to an expectation of the mandating authority to take ownership of the security, but that expectation might also extend to any mandated system. For example, a user who feels forced to use a technology will believe that the innovation or technology will be

inherently secure, rather than relying on the user (in this case someone who considers themselves as a distant third party) to initiate security-based actions to protect their online security. Similarly, but at the other end of the spectrum, a user of a mandated technology who already knows that their own skills in online usage and security are limited, will normally revert to the more knowledgeable authority (under mandated conditions of usage).

Figure 4.4 describes how one can view technology usage through a lens of mandated usage and free choice. The two types of ICT engagement, (voluntary and mandatory) move in opposite directions to each other. There is no point at which free choice usage and mandated usage intersect.

Voluntariness and Choice

Trust through usage can be affected by choice

| Mandatory Use | Imposed Use | Freely Chosen Use | Rejected |

Trust with Choice
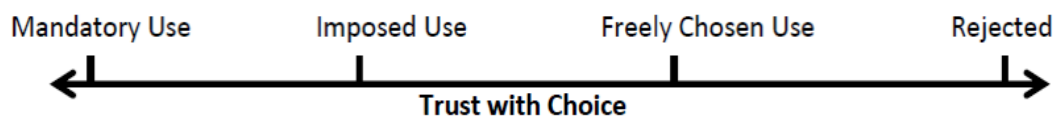
Figure 4.4 A continuum of trust, voluntariness, and choice.

There are two relationships that should not be confused. The relationship we look for is where we can describe trust and acceptance against voluntariness. Figure 4.5 explains that as technology usage shifts towards a mandated usage, it can be in either a state of trust or distrust.

Acknowledging Trust and Usage

Trust

Mandatory Usage

Free Choice to Use

Distrust

Technology can be used under both trusted and distrusted conditions, and users can choose or be forced to use.
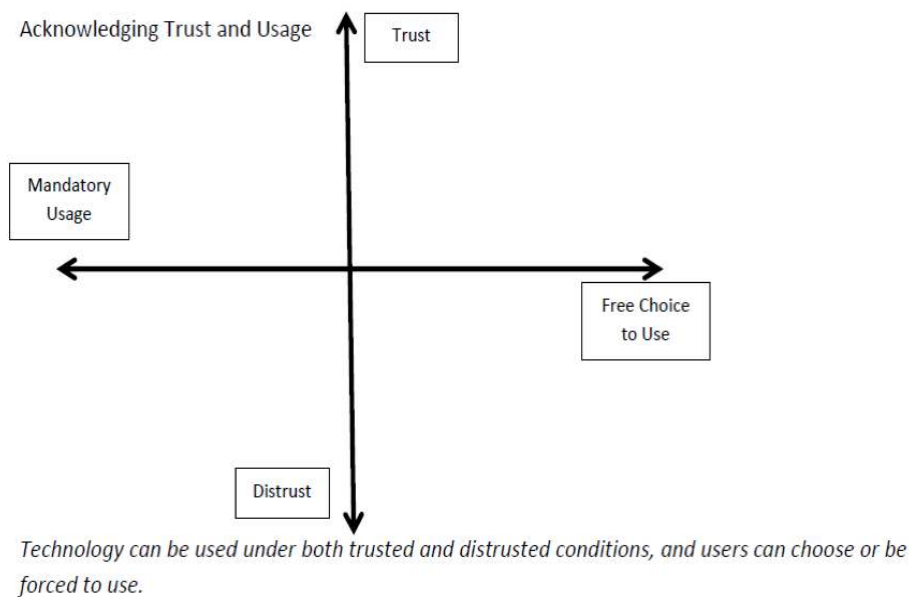
Figure 4.5 Two-dimensional continuums of trust, distrust, choice and mandatory practice.

This may, however, be confused with an acceptance that a new technology is being used (ie where there is no free choice (see Figure 4.5). At this point the relationship is not about trust and distrust – it becomes about acceptance and rejection. The relationships surrounding trust seem clear in isolation, but are more accurately considered with the addition of values and beliefs.

Whilst we can consider trust and distrust as two opposite extensions of a graph that considers mandatory usage against voluntary usage, the overall picture is too simplified to provide a useful depiction of the trust and volition relationship. Only once we add additional values, norms and beliefs, can we see that volition runs from the mandatory direction to the free choice direction. At the same time, usage is better explained as usage at one extreme, and non-usage, or rejection at the other (Figure 4.6).

From here we now have a graph that shows us four quadrants that portray volition, usage, and a variety of norms and values as variables that can shift from one quadrant to another. The four quadrants consist of Usage / Mandatory Usage, Usage and Free Choice to Use, Rejection and Mandatory Usage, and Rejection and Free Choice to Use (Figure 4.6). As different norms and beliefs are applied to a given situation, it is possible to understand the expected behavior when the type of usage is understood against the consideration of volition.

In the case of the Usage / Mandatory Usage quadrant, expected behaviors could include Resignation, Surrender, Sacrifice, and Recklessness. These behaviors apply to situations where a person is under the operating conditions where technologies are mandated. In the case of the Usage / Free Choice to Use quadrant, expected behaviors include Trust, Confidence, Reliance, and Dependence. These behaviors apply where there is usage (non-mandatory) and where there is free choice. This quadrant displays the greatest level of optimism.
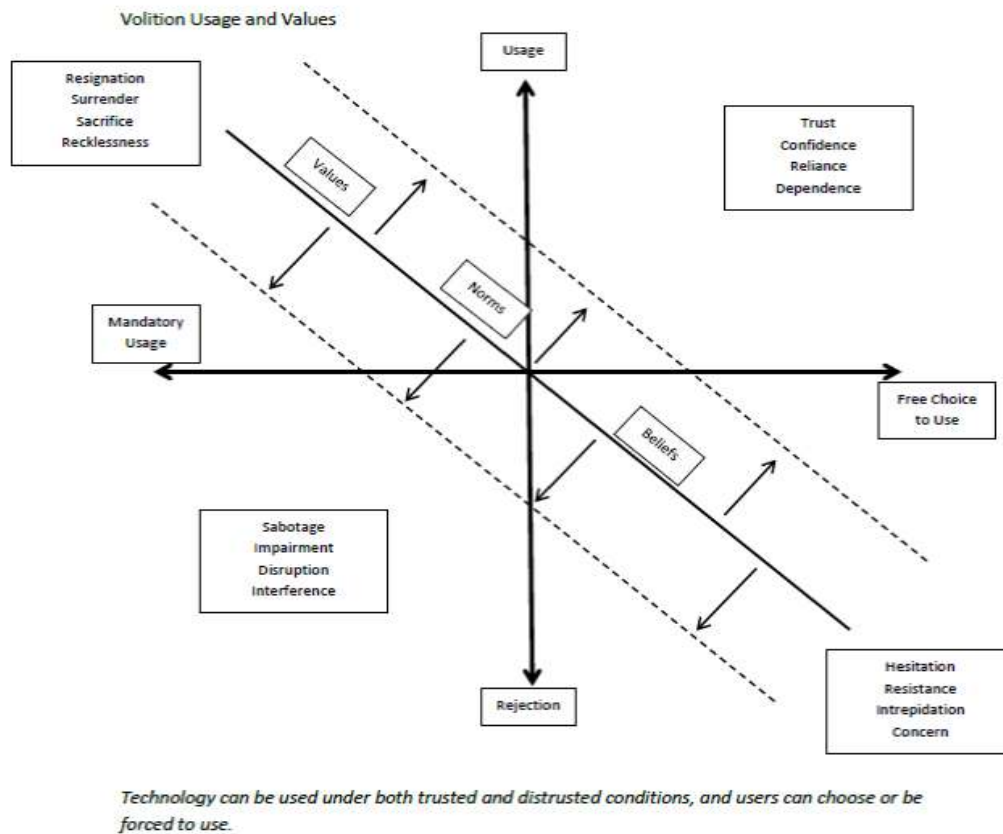
Figure 4.6. Usage and Freedom chart with behaviour variables, user belief, and norms and values.

In the case of the Rejection / Free Choice to Use quadrant - the expected behaviors include Hesitation, Resistance, Trepidation, and Concern. These behaviors anticipate that where the usage is rejected, there is still some form of uncertainty, even if the choice to use a technology is a free one. Finally, in the case of the Mandatory Usage / Rejection quadrant, the expected behaviors include Sabotage, Impairment, Disruption, and Interference. This quadrant has the most pessimistic characteristics. Where systems retain the mandatory usage, and whilst the usage axis shows rejection rather than usage, we can expect problematic behaviors to become known.

4.4   Conclusion

Thus the relationship between trust and volition goes beyond mandatory and free choice. By extending the idea to include a state that can be both mandatory in usage, and rejected in application, it is clearer to look at these two conditions through the addition of the relevant norms, beliefs and values. We now have a set of characteristics that we can consider against individual behaviours so that volition

can be more accurately considered in a scalable form, ranging from mandatory use, through imposed usage, and towards *Free to choose* usage.

The relationship between volition and usage is not clear when examined as two isolated features of technology. It does, however, look more accurate once values and beliefs are layered over the main axis. What does seem clear from the literature is that ICTs and technologies inherently impose change. Whether it be from the security perspective of new passwords, new configurations, and new anti-virus updates, or the expectation to keep up with new hardware, new smart phones, and new devices, or the obligation to shift from one program to another, regardless of whether the original program is performing well, the resounding message from the various corners of the research area is to expect change, to follow change, and to engage with new innovations, repeatedly. The message is reiterated with ubiquity at the expense of what appears to be a fundamental set of choices. The choice not to change, the decision to keep doing things as one has done them before, and the opportunity to reject or refute new technologies, new ideas, and new methods, is far less prominent in the literature, and has been far too rapidly ignored from the attempts to make sense of the problematic challenges of trust and security within a digital environment.

4.4.1   Research Outputs

The review of literature indicated a dominance of TAM-based thinking that automatically linked usage with acceptance. This research indicates that the direct linkage between usage and acceptance is a step too far, and that the role of choice plays a much greater part in trusted acceptance than the literature bears out. From an overarching view, there are minor, occasional attempts to include voluntary actions; however they are too few, and almost always presented as secondary variables of influence, rather than a mainstream concept which embeds freewill, choice and rejection as legitimate and unambiguous prima facie options.

By observing the direction and progression of TAM modelling as the dominant element in the technology acceptance body of knowledge, it is apparent that a need exists for the direct inclusion of volitional and mandated determination. TAM models show strong relationships with acceptance and

usage, but far less so when the consideration is about "trusted" acceptance and usage. Based on these observations, the need to ask older users about their trust in the use of ICT appears as the next logical step in defining the importance of volitional and mandated determination. When considering the perceptions of older people who might be attempting to engage with ICT-based financial systems such as online banking, the commercial environment that drives imposed and mandatory practices is likely to forego a comprehensive selection of ICT choices in favour of commercially viable routes of ICT usage that are predetermined and limited.

Observation and analysis of the security literature suggests that older people are more vulnerable to financial attacks through the usage of online banking than other age cohorts. A number of reflections about the nature of capability and training for older people suggest that it is not necessarily a factor of age that elevates these vulnerabilities as much as the change from working life to retirement. The shift to older environments through retirement brings about different sets of peers, learning in isolation, and distancing from the wider interactions of business and working life.

4.4.2   The following AR Cycle

Reflection of the key points of discussion suggests the need for elevating the importance of choice and volitional determination into the interview and scenario-based data collection. Reflection also suggests the need to investigate the learning, training, and capability components of older people attempting to engage with ICTs, especially their early and formative experiences, which form the foundation for their ICT usage and their perceptions of trusted and secure ICT acceptance. Two main sets of actions are put forward as a result of this cycle.

1.   Interview questions and hypothetical questions should directly confront and contest the idea of how, if at all, usage translates into trusted acceptance.

2.   Participants should be asked to describe their views about the need to trust ICTs

3.   Participants should be given an opportunity to explain different types of trust, especially in terms of delineations between trust of people and trust of ICT systems.

4.   Interview questions should examine novice and formative experiences in relation to trusted usage.

5.   Interview questions should examine usability issues for older people.

6.   Interview questions should examine accessibility issues for older people.

7.   Questions should include opportunities to compare situations involving choices, imposed conditions and mandatory conditions governing the use of ICTs

The next chapter discusses the research design, the approach taken to interviews in terms of segmentation and order, and issues relating to confidentiality, security, and the rights of interview participants.

5 CHAPTER 5 RESEARCH DESIGN, INTERVIEW BREAKDOWN, CONFIDENTIALITY AND LIMITATIONS

5.1 Introduction

This chapter explains the design of the research interview questions, and the way in which a rich qualitative data set was sought by means of a segmented interview approach. The chapter explains how a participant sample was obtained, and why a purposive sample was chosen. It explains the progression of the interview questions through a range of inquiry segments that ended with a set of hypothetical interview scenarios. The chapter discusses the limitations of this type of study, and explains how different restrictions were treated in order to reduce the impacts of bias and other limitations upon the study.

Prior to commencing the collection of data, the Human Research Ethics Committee (HREC) of Edith Cowan University (ECU) granted approval for this research, which consequently meets the requirements of the National Statement on Ethical Conduct in Human Research. Although a review of the literature is a formative part of this research study the principal data was collected by means of interview.

5.1.1 Selection of Participants

A selection of thirty-two older people participated in interviews as part of a study to determine issues of trust, decision making, acceptance and rejection of online technology. The older people were aged between 60 and 75 years of age, with an equal number of male and female participants. This provided a considerable amount of information in detail regarding older people and choices made under imposed and mandated circumstances.

Participants were selected by means of a purposive sample. The process of recruiting participants was undertaken by means of a homogenous sample of participants all over the age of between the age of 60 and 75 years of age; specifically those participants who considered themselves novice or beginner level in terms of their knowledge and usage of ICT. The sample was taken from

four senior citizen associations within Western Australia. The associations then provided lists of names of people who indicated that they would be available for individual interview.

Purposive sampling does not require a specific number in the way that quantitative sanpling does. Instead, the emphasis is placed on using information-rich questioning (Strauss and Corbin, 1990; Bernard, 2002). Purposive sampling is a system that is often applied to small sample groups. A sample size of 32 participants was chosen. He sample number was derived by examining the sample sizes recommended for qualitative research that sought to obtain rich data from participants by means of comprehensive interviews. Three research approaches were compared. In a study by Mason (2010), the mean sample size for Action research in PhD studies was 23 participants. The same study showed that the mean number of participants for Emancipatory Research was 35 participants. Additionally, the mean number of participants for Case Study research was 36. Taking these numbers as indicators of range, the sample size for this study was initially set at 32.

Qualitative research can be measured in terms of reaching a point of saturation. Under these conditions whilst an initial number for the sample is set, it understood that further participants can be recruited if there is a need to obtain further knowledge, and if it is clear that new data is being obtained with successive participant interviews. Similary, under saturation conditions, the number of interviews and the sample number may stop at an earlier point, if it becomes clear that no new significant data is being obtained by further interview participation (Galliers, 1993; Palinkas, Horwitz, Green, Wisdom, Duan, and Hoagwood, 2015).

In this case the specific aim was to deliberately find participants who were within the specified age range and who could be classified as novice in terms of their ICT experiences. The number was derived from three main criteria. The sample number should include an equal (or close to equal) number of participants from each of the four purposively selected aged associations. The sample should target people who had little ICT experience.

Table 5.1 Data collection, breakdown of older participants from older peoples' associations

	Number of Female Participants	Number of Male Participants
Association A	4	3
Association B	4	3
Association C	3	4
Association D	3	4
Total Participants = 28	14	14

This sample was formed by ordering by name and then the names on each of the four association lists were randomly selected from within each separate association. Participants were selected using alternate gender selections from every fourth person so that the first list's fourth female, was selected, and then the fourth male was selected and so on. This produced a list of thirty-two participants. From this list twenty-eight were selected based upon satisfactory alignment with the participant criteria. Four participants were excluded from the original group of 32 subjects after disclosure of high-level ICT experience and long-term ICT usage. The participants formed a selection of fourteen females and fourteen males (Table 5.1).

5.1.2   Interview Design

The in-depth interviews were undertaken in order to gain an understanding of ICT interaction and engagement centred around security issues as well as daily usage where security issues might be expected to arise from time to time. Participants in the interviews were required to answer fifty-seven questions. The interview questions were arranged into five sections (Fig 5.1). The data provided direction and insight into the impact of technology upon ordinary everyday tasks and practices that have changed "over time" from paper-based systems to online digital practices.
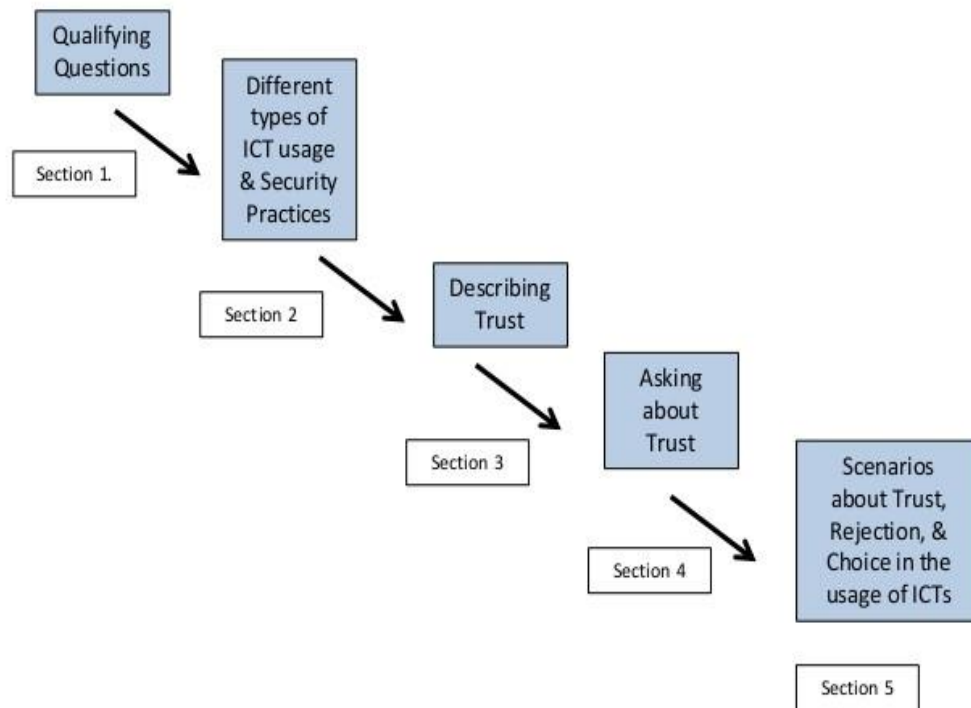
Figure 5.1 Interview segmentation and progression

Section one used nine questions to confirm their suitability for the study. They were used to establish participant's levels of ICT usage and experience. The study aimed to interview participants who considered themselves as beginners, and who were in a class of user that implied some tasks were relatively novel. Questions inquired about age, working status, internet usage, email and online communication capabilities, and training undertaken (both formally and informally). This section asked a set of non-technical, jargon-free questions in rapid succession, with no participants exhibiting hesitation or confusion during the section.

Section two asked participants in more detail about their daily or regular internet and computer-based engagements. Participants were asked to explain the process by which they navigated to emails, and to explain how they went about using and managing their emails. These questions extended to send and receive functions, email storage and management, and email deletion. The section also asked participants about their password habits, ascertaining those with password protection across applications and those who felt little or need for password protection. The participants were also asked

155

to respond about those applications where passwords were required as standard operating conditions, such as in the use of internet online banking. The participants were also asked to explain their perceptions about the ease of use of their varying applications and programs, and asked as to whether some applications would be used more regularly if they were easier to access and use. The questions explored money transactions in both online and face to face conditions. These questions tested for perceptions regarding the secure movement of money in both online and physical conditions. Participants were asked a range of questions relating to their understanding of anti-virus usage, vulnerabilities, and whether they felt they had experienced some form of malware, social or physical exploitation, or some form of online deception.

Section two uses a set of twenty-two questions to get a deeper understanding about their communications usage, their financial usage, and perceptions about differing hardware technology, predominantly the difference between personal computers, laptops, and more mobile devices such as smart phones and tablets. Participants revealed a range of online and physical habits surrounding financial needs including ATM access, physical face to face bill paying, online bill paying and the transferring of money (both online and through agents).

Section three asked participants five questions about their levels of comfort and trust in their use of computers. Participants were asked their perceptions about ease of use and perceived usefulness in online financial transactions including banking, online purchases, and the ability to use and trust new financially-connected systems and applications. The participants were then asked to respond to a range of questions about their trusted use of new technology software and hardware, ranging from popular social media applications to banking applications, and including their perceived trust of new mobile hardware devices (smartphones and tablets) for the secure storage of private information including financial information. The section asked the particpants to reflect on their own technology interactions in an attempt to gauge technology trust.

Section four asked participants nine questions where they could consider both the accepted usage of technology and also the possibility to reject the technology in preference of a non-cyber alternative. The respondents were asked about situations where they used technology slightly outside of their own comfort zone, such as the use of someone else's computer, or a public computer for a

financial transaction. Participants were asked to explain their perceptions and judgements about what constituted a risky transaction, and under what circumstances a transaction might become less secure. Participants were asked to explain their thinking about the confidentiality of their information and about their email correspondence. They were asked a range of questions relating to third-party interactions, and what levels of security and trust were tolerated. The questions involved the levels of trust connected with the usage of someone else's hardware, and about the use by others of the respondent's hardware. The questions also examined the use of social media under shared circumstances. The participants were asked to explain their outlooks about their trust of systems and applications (both online and physical) whose usage was suggested by others. The questions collected a range of information about decisions to trust or reject the use of technology. They also included broad issues of usage where the interactions were obligatory rather than voluntary.

Section five used a range of scenarios presented to the participants as possible situations where choices regarding technology usage, acceptance, trust and rejection were up for consideration. There were twelve scenarios put to each participant. The scenarios included a range of mandated and obligated scenarios. Participants were required to offer choices as to how they would react in circumstances where the key element required access and acceptance of an online system. These scenarios included a full shift to online banking, use of online systems for pension and funds access, access to international airfare ticketing, phone banking, and hotel bookings. Participants were also given scenarios where the use of an online system was not necessarily mandated, but was obligated. These included perceptions of trust regarding other persons who were using mandated systems that had an impact or affect upon the participant. Some scenarios required a transition from an existing trusted system to a new system, whilst others cited third party experiences where the participant was not asked to consider themselves as the direct user, but instead as someone affected by the use of a digital system whereby trust was brought into question. The fifth section was considerably longer that other sections. Participants needed time to consider each scenario before giving their responses. Each scenario had an historical connection that related to the way something was done in an era that pre-dated ubiquitous systems in ICT.

Each scenario in this section had an historical association that related to the way something was done in an era before ICT ubiquity. Participants were asked to explain their likely actions and reactions

157

to the scenarios as well as their perceptions about each scenario. The twelve scenarios depicted instances where ICT usage ranged from implied, to obligated, to mandated. Participants were given several minutes in to answer in this section, as some responses required a carefully thought out response, and participants were actively engaged in accurately describing their opinions.

5.2 Confidentiality, Security and Rights

In order to ensure adequate security and safety of the confidential interview data, the transcripts were retained by the researcher, who was the only person with access to the transcript material (apart from the researcher's supervisors). All participants read and retained a copy of a consent form outlining the ethics approval, confidentiality, and security of the interview material, and its associated transcripts. All of the signed consent forms, participant information, and recorded material was stored in a lockable filing cabinet in a secure locked office within Edith Cowan University.

All of the respondents were advised of their rights in regards to the interview process, and the usage of the interview data. They were specifically advised that the information would be anonymised, that they could withdraw at any time, and that they could access their individual transcripts to ensure accuracy and truthfulness after the interviews had been recorded, transcribed and available in printed form. Each respondent was given the opportunity to see their transcript, and to advise if they felt that there were any breeches of privacy or confidentiality in the transcripts. There were some respondents who took the opportunity to review their comments and asked for some changes, citing in some cases that they had not made themselves clear. None of the respondents asked to have information removed, and in all cases respondents confirmed that the transcripts were a true representation of the information recorded at the time. Every respondent reviewed their individual transcript. None of the respondents saw any other transcripts other than their own.

5.3 Limitations of the study

In the approach and the research design planning, a number of limitations were identified with the intention of mitigating their influence over the study. One of the first of these limitations repeatedly

appeared throughout the process of selecting potential respondents for the interviews. Those older people who are most interested in volunteering for interviews around technology and ICT-related affairs were also the same people who have been actively involved in engaging with ICTs more regularly and more enthusiastically than others. Whilst not all of these volunteers were skilled in the use of digital technology, a great many possessed a high level of skill and technology acumen in dealing with challenges relating to the trust and use of ICTs. It was observed that on several occasions some volunteers' enthusiasm to be involved in the study overshadowed their honesty and truthfulness in acknowledging their more highly developed and regular ICT interactions. The ideal respondents needed to match the profile of a novice or beginner in the use of ICTs. Thus those volunteers who were already working in part-time paid capacities as ICT trainers were ineligible and inappropriate candidates to be interviewed. Whilst it might not be possible to know if a person successfully and deliberately falsified their individual statements about their ICT skill and knowledge, the qualifying questions were useful in establishing a baseline of suitable respondents. One of the participating associations initially wanted to only put forward a sample group of people who were actively involved in a training program that was in place. By asking for a large sample group rather than a small one, and by randomly choosing from a large sample, it was possible to mitigate against the enthusiastic attempts by associations to take a deliberative approach to the acquisition of suitable interview candidates.

The choice of participants was derived through associations of older people, and then a process of randomisation was used to finalise the respondents for the interviews. The four associations were chosen in order to attract a range of participants from different socio-economic, different geographic, and different educational backgrounds. Since the sample was purposive in nature (ie it specifically targeted novice ICT users within a specific age range), the random selection of participants to a smaller sample size is a useful strategy to reduce bias.

A rich diversity of people within the respondent group was desirable, since a determination of trusted technology use would need to cater for a range of backgrounds, where mandates, impositions and obligations have a different meaning between one locality and another. It was important that a range of diversity in user-technology could also be achieved. The literature on technology choices suggested that older people consistently hold expectations about the longevity of technology products that were

unrealistic compared to the rest of society (Haddon, 2000, Xie, 2003). One limitation in this regard is that some older people cannot afford the cost of technology. Thus whilst attempting to draw from a rich and varied sample, it is likely that some exclusions take place because there are older people who have no understanding of digital technology owing to the prohibitive cost of its purchase and interaction.

The duty of investigators, in interpretive studies, is to sidestep imposing their own constructions and to be accurate to the sagacity given by the participants (Blackledge & Hunt, 1985; Kumar, 2011). However, cultural norms and/or bias of the investigator can sway what is asked and what is heard (Rubin & Rubin, 2005). One limitation that restricts the quality of the responses is the very jargon-laden terminology which pervades digital technologies. The computer science field uses many acronyms, and also uses words and terms that may not be in common use in everyday language, but which are saturated into many discussions involving digital technologies. The need goes beyond simply explaining acronyms from ICT to Information and Communications Technology. During several semi-structured interviews, it was necessary to explain some terms and acronyms to assist a respondent in their answer. Such explanations are problematic for at least two reasons. The first is that some respondents may pretend to understand words that appear to them as jargon, yet have little or no idea as to their meaning.

This may add to responses that are cautious and may prevent the revelation of something important. The second challenge is that by the researcher introducing some terminology from within a known digital technology vocabulary, the researcher is also introducing cultural norms and bias to the interview process. These limitations were, in part, addressed by informing each respondent that they could ask about any word, term or acronym that might have been unclear. The second point of address was in scrutinizing the interview questions and having them tested on a small group of older people before the interviews were conducted. This small group were able to identify a range of terms that were either ambiguous or unknown by those checking the questions.

This was in line with the limitation being identified in the literature review in the first research phase. In a study of this nature, bracketing and suspending judgements or assumptions can be used to highlight the subjective meanings of the participants' actions (Christ & Tanner, 2003; Denzin & Lincoln, 1994). The investigator's task was to interpret by what means others understood their domain and to think through the meanings behind their actions (O'Donoghue, 2007).

An interpretive approach such as the one described here has the potential for personal bias (Guest, et al., 2013). In order to reduce this effect a reflexive process was included in the approach to evaluate bias during the data interpretations (Bednall, 2006). This was established through maintaining a research-focused reflective journal, which recorded considerations to after each interview. This journal kept a record of observations, discernments, and interpretations of the material offered by each respondent (Gall, Gall and Borg, 2007). It allowed for further comparisons from one respondent to another in areas of commonality, or opposition. The journal included an analysis of each interview process, developing an understanding of relevant background and circumstantial information that was either apparent or observed. The journal was a useful assistant in the recall of specific details and explanations from respondents during each interview. These details made for connections and linkages to other information that might otherwise have remained in isolation.

An additional limitation was the use of associations for the purpose of acquiring respondents for the interviews. The interview respondents were drawn from four seniors associations, however the question could be asked as to whether associations are appropriate places to draw respondents from, and whether they would provide a sample of people from a wide and varied sample of older people for this study. It could be argued that since associations are inclusive organisations that deliberately share information across a range of older people's interests, this study cannot be seen as representative of all older people, some of whom may lead very secluded and lonely existences. Older people who are members of associations are by definition of their association membership more active than others.

This study is an example of purposive sampling, since the choice of older people was deliberate in terms of looking for respondents who met the inclusion and eligibility criteria for this study (Patton, 2002). In this case, a sample included older people within a specific age range who were retired. The eligibility criteria were operationally enforced in order to bring about a specific sample group of respondents (Bernard, 2000). Thus purposive sampling techniques cannot be seen as being representative of all older people (Patton, 2002).

The sample group of respondents were all volunteers. As a cohort, the respondent sample was found to be assured, coherent and articulate. They volunteered and attended at specific times, indicating a level of mobility, freedom, and availability. This suggests that there could be some respondents who

have been excluded or marginalised from this study. This study is limited in that it did not interview people with mobility or accessibility issues, and it did not specifically include older people using assistive technologies. There are older people who may have been unavailable, or who lacked the confidence or desire to participate. This study, therefore, is not accurately characteristic of all older people and their interactions with trust and technology.

This study included interviews that took a significant time to complete. The shortest interview took 24 minutes and the longest interview took 58 minutes. The length of time each interview took meant that the interview process may have precluded some older people from being involved on the basis of time. Thus the study was limited to those people in both reasonably good health and with a reasonable amount of mobility. Availability was a factor in the selection of the final sample respondent group (Seidman, 1991; Guest et al, 2013). In some cases, the researcher adopted a method of availability and timing flexibility to reduce the unavailability of respondents who had been initially selected through the original method of sample selection. The limitations in regards to length of time were addressed individually with each respondent. All respondents were asked if they needed a break, or extra time. There were two instances when time breaks were included so that one respondent could take a comfort break, and so that a different respondent could take a rest. Potential respondents were reminded that interviews would take a portion of time. In the case of initial volunteering, potential respondents were told that the interview would take at least 20 minutes, but that they were not likely to go for more than one hour in duration.

Initial analysis of the data was guided by the research questions. The analyses of the data therefore included the personal bias retained by the researcher, who has previously interacted with older people on matters of online cyber security. In cases where the researcher has been involved in the subject matter of a qualitative study it is important to recognise and mitigate bias that is retained from prior knowledge (Kock, 2004). For example, the interviewer might unknowingly frown when an unexpected answer was given, or where the act of nodding as a respondent answered a question might be interpreted as a seemingly appropriate answer when in fact the interviewer might simply be nodding to acknowledge that the words are understood (Jackson 2009). Thus it is necessary to disclose that there is residual bias that remains connected with this study as a result of the researcher's previous

interactions with older people on issues relating to cyber-crime and trusted online technologies. This limitation was mitigated by asking other people to read and assess the interview questions for any signs of bias or partiality. The interviewer took care to avoid unnecessary eye contact and restrict facial expressions when interacting with interview participants.

5.4 Summary

This chapter explained the way in which the research was designed around a small purposive sample of 28 participants who were interviewed across five areas of interest. These five areas formed segments that gathered information about suage, acceptance trust and technology rejection. The first segment considered suitability, asking questions relating to basic usage, and establishing the limited range of experiences within the participant cohort. The second segment examined a more detailed understanding of usage, looking at online navigational practises, email managemenmt, password behaviours, and both physical and onbline financial transactions. The third segment examined comfort and discomfort around perceptions of trust and new technology, and the usage of financial and transactional systems. The fourth segment considered the acceptance of usage involving other people's systems, software and hardware. It looked at 3rd party transactions, and a range of trusted and rejected systems used for financial transactions. The fifth segment explored detailed descriptions about hypothetical scenarios that examined trust and rejection under difficult or uncertain practises involving change and acceptance of online systems.

A description of the research design and techniques for this study was incorporated. It included descriptions about participant information, ethics, data collection and the processes adopted to analyse the data that was obtained.

In the closing parts of this chapter, the limitations that pertained to this study were explained and clarified. This study aimed to capture and to understand the knowledge, norms, practices, and experiences of older citizens in the adoption, interaction and rejection of technology pertaining to trust

and trusted relationships. This required the investigator to obtain the perceptions of older people by means of a descriptive process involving the acquisition of rich understandings using insights, discernments, and observations.   The next two chapters present the results of the data collected, and present those results in the form of a set of findings based on interviews with older people.

6   CHAPTER 6   DATA AND RESULTS FROM INTERVIEWS

6.1   Areas of Inquiry

The purpose of this study was to investigate the nature of trust in technology within mandated and imposed settings by older users of online digital technology. To achieve this, twenty-eight older people were individually interviewed about their online interactions. Each respondent was given an interview comprising of fifty-seven questions relating to their experiences with online technology. Questions focused on trust-based relationships where users were expected to trust a new system or technology using online systems. Some of the questions tested for experiences that came about through voluntary exposure to technology, whilst other questions looked at user experiences where the online technology trust was either imposed, obligatory, or mandatory. Participants gave their answers verbally, and their responses were recorded using a digital recording device, which was later used in playback as a means of obtaining a transcript for each interview.

Table 6.1 Areas of Inquiry

Areas of Inquiry	
Part 1 Interviews	Basic Proficiencies
Part 2 Interviews	ICT Usage & Interaction
Part 3 Interviews	Perceptions of Trust in Money and Information
Part 4 Interviews	Rejection and Limits of Trust
Part 5 Scenarios	Hypothetical Scenarios

The questions were partitioned into five main areas of inquiry (Table 6.1). The first part tested respondents to answer questions outlining basic proficiencies in the use of ICTs. The second part looked more closely at each respondent's usage of, and interaction with, ICTs. The third part asked participants about their perceptions of trust in relation to items of value such as money and information. The fourth part looked more closely at issues of trust by aiming to measure each respondent's limits in determining when to trust or when to reject a given ICT technology. The fifth and final part of the interview process asked questions centred on specific trust-related scenarios. This is discussed in chapter seven. The responses provided many insights into the way older people perceive technology and trust, and the

differences between trusting ICT systems where there is little or no alternative, as opposed to scenarios where usage and its accompanying requirement for trust, were not mandated. The interview questions were put to the participants and their answers were recorded, transcribed, and noted for the study.

6.2   Interviews Part One - Basic proficiencies

The first part of the interviews examined areas of fundamental online activity. It established whether the respondent in each case was typically a novice user of ICT and that they used the Internet and were active online. This first section asked respondents to demonstrate their capability to use email, and to address some areas of digital communication proficiency. The section also examined previous training, and whether the respondent saw them as a novice, or whether they perceived themselves as having a more developed aptitude, capability, expertise or skill.

6.2.1   Email as a capability reckoner.

Findings obtained from analysing the data showed that older people understood the concept of electronic mail (Table 6.2). The responses showed not just whether a person could or could not send an email, but also revealed where there was uncertainty.

Table 6.2 Email themes

Email Themes	
Confident in sending email	78% Yes – self assured, 22% Some help needed
Able to get an email sent	96% Yes – self assured, 4% Unable to send email
Uncertainty about how to send email	53% Some uncertainty, 47% Confident to send

32% of respondents knew how to find and press the send button on an email system that was set up on a mobile device such as an iPad, but that they might not be able to retrieve emails from other devices such as a desktop or laptop computer. Of these respondents 93% cited the need for someone else to set up or install a system on to the desktop screen before they would feel confident to send or receive emails on a different system to their own. *"Well as I said, I have very limited knowledge. So when my friend comes over we sit at the computer and she helps me to get into the email section and*

we go from there. Once I'm in I can find the emails quite easily. But getting started is a bit of an ordeal I'm afraid". (Respondent 20).

The majority of responses (78%) indicated with confidence that they were capable of sending emails. However, none of the respondents showed any ability to articulate the method by which they sent the email. "*I use an iPad. I open the app, and access my emails from there. I can send replies, store emails, and delete the ones that I don't want to keep* (Respondent 25). 96% of responses indicated that they could send an email. Only one response indicated their inability to send email.

There were 53% of responses registered as showing hesitation, confusion, or over simplification in the task of sending an email. Whilst some respondents cited an ability to tap on the "mail" icon on a tablet or mobile device, other respondents cited the need for assistance. Respondent 4 stated "*Um yes – well I know the theory. Sometimes I find it hard to get to where the emails are. I have a couple of friends that help me out … the thing is that one friend will show me one way and another friend will show me a different way altogether… it very confusing".* Similarly, Respondent 10 voiced her concern, "*but I'm not sure if I'm doing it the right way".* Whilst Respondent 17 explains "*Well I turn the computer on and I go to the Bigpond page and go to the emails".* Two respondents stated that they understood the theory behind sending mail even though in reality they had never sent an email. One clarified his limitations when asked if he knew how to send an email … "*Well, um, not really, but if you set it up for me then I can type in a message. I always get help from my friends at the seniors group".* (Respondent 12)

Whilst 78% of the respondents claimed they were confident in sending email, only 47% demonstrated genuine proficiency, whilst more than half of the respondents had misunderstandings or hesitation when asked specific questions relating to the actual process of sending an email. Some respondents showed confidence in their device to send communications even though they did not understand a method by which to send an email. Others were reliant upon clicking an application that did not require them to understand the email sending process.

6.2.2   Previous training involving Information Technology

Questions about previous training can help indicate the general skill levels, whilst specialist training (Cyber Security) may indicate needs-based interest over and above the majority of respondents who had either had no formal training or had undertaken simple Microsoft courses and iPad courses (see Table 6.3).

75% of participants indicated that they had either no previous training or were definitely still in the class of 'beginner' in terms of using a computer. "*Yes I've done a couple of afternoon one-hour workshops with seniors and I did the One Click program at Mirrabooka.*" (Respondent 4). Of the remaining respondents the previous IT training ranged from half day 'iPad' courses to one-day beginner courses focusing on the instruction of Microsoft programs such as Word and Excel.

Table 6.3 Previous Training.

Previous ICT Computer Training	
Beginner, Novice, little or no substantive training	75% No substantive training, 25% Some training or an ICT course
Microsoft Training (Word, Excel)	81% of those who attended a course did Microsoft training, 19% no training or generalised introductory training.
Cyber Security Talks	12% Yes – attended Security Presentations, 88% No Security training or cyber talks

One respondent cited having undertaken a two-day specialist course for senior citizens at a free course that was run as a church-based outreach program that had developed a series of IT workshops. "*I've gone to a few computer talks and seminars run by the (seniors) association. There is an annual seniors' conference each year, and there is always someone who presents on computers and technology. They are always talking up the need to change your password regularly so that you don't get your identity stolen and your computer hacked*"

(Respondent 11). Of those who had attended courses more than 81% of them had either undertaken a course in using Microsoft Word or Microsoft Excel. The overall level of training and education was very low across the entire cohort. "*Oh I'm definitely a beginner. I mean I've been doing emails for a few years, But I don't really know how the machine works, or how to get the most out of my internet searching. I'm pretty hopeless I'm afraid*" (Respondent 11).

6.2.3 Previous work before retirement

Respondents were asked if they were currently retired (or not working) and what kind of work they had done previously. The respondents indicated that they were no longer in a working capacity. The question had two purposes. Firstly, it was important to ascertain whether any of the respondents were still working, since that would possibly affect their likelihood of a greater developmental ability in using ICT.

Table 6.4 Previous Employment.

Previous employment and interaction	
Previous need for ICT usage and ICT skills	47% Yes – Needed to use ICTs in work, 53% No – employment skills did not require ICT skills.
Felt they were too old in their job to learn to use a computer	29% Yes – Too old to take up ICTs whilst at work, 71% Did use computers during last years of employment before retiring.
Homemaker / housewife with no computer usage in life before retirement	11% No work history with ICTs (Informal – no recorded work history) 89% Held a formal job from which they retired.

Since no participants responded that they still had work, the question relating to previous work allowed some understanding of the diversity of the interview cohort. The respondents fell into two roughly even groups (Table 6.4). Approximately half of the respondents (53%) cited a previous area of work that might *not* require specific IT skills if undertaken today. These respondents were from a broad cross-section of the labour force and included: a gardener, a food handler in a delicatessen, a cleaner, a tea lady, a postman, a golf club roustabout, and three housewives / homemakers. Of the remaining respondents (47%) there was also a broad cross section of working positions, however these were in areas that *would* require IT skills if undertaken today. These included: A Police Officer, a Centrelink clerk, a manager of a hardware store, a worker in the Australian Air Force, a personal assistant for a mining executive, a public service administrator, a book keeper, a stock-take specialist, a library technician, a newsagent, and a primary teacher. Respondent 17's answer was typical of the replies…: "*I'm retired now. My husband and I ran the news agency in Booragoon for many years until 2001*". Similarly, respondent S1, was representative of a working life that held little previous need for IT. "*I was a homemaker. My husband worked as a bus driver, and I stayed at home.*" (Respondent 20).

Some respondents also cited regret in not learning to understand more about ICT during their working lives. *"I was the manager of a hardware store for over twenty years, but I resisted the urge to use computers until I was at the end of my working life…. And I think I left it a bit too late."* (Respondent 7). 11% of respondents cited being too old, or leaving things for too long is evident through many of the interview cohort's comments. Older people demonstrate a perception that it's too late to learn at their age, and that they could not possibly hope to catch up to the level of others. They describe that ICT has now become so much more complicated than before. *"If they need checking, then my daughter can do that. She set the email up for me in the first place. I don't look at them, it's too convoluted. None of them are urgent so I don't bother unless my daughter comes over to see me."* (Respondent 5).

6.3   Interviews Part Two – Usage and Interaction

The second section of the interviews examined the types of technology usage that each respondent had some experience with. It asked questions about hardware and software, and ascertained what level of technical knowledge they had. This section also asked respondents about password usage, asking them to explain the number of different passwords that they had, if any, and any associated issues that passwords presented.

Those interviewed were also asked about communal password usage and usage by others, and why, or why they did not, share passwords with others. Additional questions included queries about their communications practices. The aim was to establish whether their communications were reliant upon postal mail and face to face communications, or whether there was confidence in the use of email and online communications. The questioning extended beyond simple email communications to include Web 2.0 interactive options including social media, YouTube, and LinkedIn usage. There is a breakdown of the interview questions as they are discussed in each subsection.

Other questions examined fundamental Internet and World Wide Web access, as well as understandings about smartphones, tablets and other mobile devices. Participants were asked to recount their banking and bill-paying regimes using online systems and over the counter payment customs. In each instance respondents were asked to explain which systems held the higher level of trust, and were asked to explain their thinking in choosing one system over another.

6.3.1   Frequency of Usage and Interaction with Email Communications

Responses to email communications and the comparison to postal mail communications revealed differences between the two communications medium (Table 6.5). Findings showed that 40% of respondents indicated that they checked their emails daily. By the same token, 38% of respondents indicated that they checked their emails in an ad hoc fashion. Respondent 4 told of how often she checked her emails: "*Not very often. I'd like to check them more often, but I'm really just too old to do this properly. It's just getting into the email part that stops me*". Respondent 20 indicated that the checking of emails was a social exercise: "*I check my emails only when my friend comes over. Then we use the computer together*". Some stated that they were not concerned, and would check them when they remembered. Respondent 18's reply was: "*When I get around to it, it's not a regular thing*". Others also said that they would look at them when they remembered, or when they got around to it. Some respondents said that they needed to be reminded by a friend or relative to check them. Nearly 20% of the respondents cited that they checked their emails once a week, or unless directed to check an email or prompted by a third party.

Table 6.5 Email regularity and interactions.

Frequency & Interaction with Email	
Check emails every day	40% Yes, 60% No
Had a regular routine for checking emails	38% No – checked them when they remembered. No specific regular practice, 62% Checked emails at regular intervals (eg: Daily Weekly)
Checks letterbox every day for postal mail	97% Yes – check it every day, 3% Not every day but several times a week

More than 60% of the respondents to this interview perceived that their email correspondence had a different meaning to their postal mail. Nearly every respondent (97%) indicated that they would check their letterbox every day looking for mail. This suggests that older people don't accept the online email form of communication with the same level of acceptance at postal mail. "*I'm not fussed about the emails; I check them when I remember. There's never anything urgent in an email*". (Respondent 2.)

6.3.2 Difficulties with the process of checking emails

Findings indicated that 18% of respondents had no understanding of how to go about checking their emails. A further 35% of respondents had only a very basic understanding of how to check their emails. However, 92% of these respondents (ie both those with no understanding and those with basic understanding) were able to describe their process of checking emails in detail. They described waiting for the computer to switch on and from there they were able to describe a process that entailed clicking on a previously established icon, symbol, or marker that was visible on their desktop or laptop screen or tablet surface.

In contrast the remaining 47% of respondents (from the whole cohort) were comfortably able to cite a range of descriptive processes, including the process of engaging a browser or URL in order to access emails from their Internet Service Provider (ISP) or another email service provider. These responses included accessing GMail, Telstra BigPond, Windows Live, and a range of Windows and Apple Macintosh environments.

Table 6.6 Email difficulties and the ability to check email.

Challenges with the Email Process	
Ability to check emails	18% No Understanding, 82% Only basic or rudimentary understanding
Had a regular routine for checking emails	38% No – checked them when they remembered. No specific regular practice, 62% Checked emails at regular intervals (eg: Daily Weekly)
Checks letterbox every day for postal mail	97% Yes – check it every day 3% Not every day but several times a week
Low level of understanding about email security	36% Low level of understanding, 64% Average or better level of understanding about email security
Trust in a Brand Name	28% Cited that Apple products were safe from email problems with Viruses and Trojans, 72% Acknowledged the need to be careful with email security.

The results showed that 36% of respondents had very little understanding about security issues pertaining to emails (Table 6.6). These respondents stated that under normal conditions, they would open any email and would open any and all attachments. "*Well I turn on the computer, and I sit down with a cup of tea and wait (laughs). It takes a few minutes, you know, to warm up, and then when it makes an annoying little tune, I know it's ready. I just click onto my Yahoo button and then I'm free to look at all my emails.*" (Respondent 11). Most respondents (82%) cited have a basic or rudimentary understanding of how emails are accessed, and viewed. The remaining 18% cited having no understanding on accessing emails.

"Well, as I said, I have a limited knowledge. So when my friend comes over we sit at the computer and she helps me to get into the email section and we go from there. Once I'm in I can find the emails quite easily. But getting started is a bit of an ordeal I'm afraid." (Respondent 20).

Respondents demonstrated a reluctance to show caution, and instead were more inclined to open emails directly. Within the subset of these direct respondents, 28% acknowledged that they felt that they could open any parts of an email as long as they did so on an iPad, citing that Apple products are inherently safe. *"I use an iPad, the prompts are very straightforward I simply touch the "mail" icon, and then read down the list of emails"*. (Respondent 8). *"Well I don't know properly. I just get my friend to help to get me into the email section, and then I can look at them. I'm not in a great hurry because so many of them are just silly things and emails from people I don't know"*. (Respondent 4).

6.3.3   Opening emails without hesitation

This question is designed to show what kind of caution and restraint might be evident in the action of opening emails without regard to whether the email was from a known source or of unknown origin. The findings show that 42% of respondents will open emails from anyone. *"I open Gmail and look for the unopened emails.* (Respondent 1). The practices of respondents demonstrate occurrences of opening emails regardless of subject matter, heading, attachments or content. *"Usually I have my machine turned off at the wall, so I'd have to turn the machine on. Then I have to log in, and then I go to my Windows, to the emails. I'm in BigPond"*. (Respondent 21).

For more than 32% of respondents, there appears to be a strong belief that the email technology is easy to use *"I have a computer, it's a great big box and I have a computer screen and a keyboard and a mouse. Oh yes it's a Dell machine. Checking email is fairly easy. I turn the machine on and go to the Bigpond section. Everything is straightforward from there. It shows how many emails I have waiting to be opened. Then I just click onto each one and open them"*. (Respondent 18).

Table 6.7 Opening emails without hesitation.

Opening emails without hesitation	
Open an email from any source	42% Willing to open from any source, 58% Unwilling to open without precautions in place.
Brand and Email set up provide acceptable safety levels	38% No – checked them when they remembered. No specific regular practice, 62% Checked emails at regular intervals (eg: Daily Weekly)
Checks letterbox every day for postal mail	97% Yes – check it every day, 3% Not every day but several times a week
Low level of understanding about email security	36% Low level of understanding, 64% Average or better level of understanding about email security
Trust in a Brand Name	28% Cited that Apple products were safe from email problems with Viruses and Trojans, 72% Acknowledged the need to be careful with email security.

Statements from respondents showed a low level understanding using email. "*Well, I don't know properly, I just get my friend to help me, get me into the emails and then I can look at them*". (Respondent 4). "*If they need checking, then my daughter can do that. She set the email up for me in the first place. I don't look at them – it's too convoluted - None of them are urgent so I don't bother unless my daughter comes over to see me.* ". (Respondent 5). "*Well as I said, I have very limited knowledge. So when my friend comes over we sit at the computer and she helps me to get into the email section and we go from there. Once I'm in I can find the emails quite easily. But getting started is a bit of an ordeal I'm afraid*" (Respondent 20). The results indicate that many ICT practices are left to others, or require assistance from others (Table 6.7).

6.3.4   Type of Device and Associated Knowledge

Respondents were asked to describe what kind of physical device they used (eg: Desktop, Laptop, Tablet, and Mobile Phone). At the same time their descriptions were noted so as to demonstrate additional awareness, familiarity, and knowledge of their devices and how to use them. The results indicated that 66% of respondents had a desktop computer. There were 32% of respondents who cited ownership of a laptop computer. Three respondents did not know what type of computer they had, except that they knew they owned a computer. Many respondents owned more than one form of device. 35% of respondents cited having either an iPad or some form of tablet. Of these respondents none thought that they had an Android tablet, though six respondents said that they had an iPad (Table 6.8).

Table 6.8 Device knowledge and types of systems.

Device knowledge and types of systems	
Multiple Devices	39% Own at least two devices (eg: Desktop, Laptop, Mobile), 61% Own a single device
Knowledge of Operating System	91% able to nominate OS (eg: Win7, Vista, XP, Win8), 9% Uncertain of Operating System
Knowledge of Brand	48% know what brand (Dell, Mac, Samsung, Apple), 52% Uncertain of Make or Brand

Within the group of respondents using smartphones 50% cited an IOS / Apple phone, and 50% cited a non-Apple phone or operating system. All of the desktop users stated using some form of Microsoft system. Of the laptop users, 68% of them had a Microsoft system running on their machine, whilst the remainder said that they were using an Apple system. Almost all of the desktop users (91%) were able to nominate the operating system that they used (ie Windows 7, Windows Vista, Windows XP, and Windows 8). When asked to nominate a brand name 48% of all respondents were able to nominate a brand (ie Dell, Mac, Samsung Galaxy, Apple iPad etc). "*I have a computer at home. It's a Celeron I think, and it has Windows XP. It's not difficult to get on the Internet (although sometimes I forget to turn the modem on as well… I sat there once for nearly an hour until I remembered to turn the modem on at the wall. Once the computer goes through all of its little checks and tests it lets me know when it's ready by a funny sound, and then I just go to Gmail*". (Respondent 7).

In some cases respondents knew what the brand of teyh computer was, and stated atht the computer was easy to use. Most respondents cited their easy of use in the form of a preset icon on their desktop, or an easy to access app that was opened by touching an icon, as in the case of respondent 11: "*The brand is Dell, and everything is pre-set. It's all set up so that I just click on the little picture and it changes the screen into the Yahoo program. It's easy to see the new emails because they are the ones still in bold. Once I've opened them, they appear in the list of emails, but they are no longer in bold. It's pretty easy, I mean I open each one, and then either reply to it or store it away for later.*"

The results further demonstrate that from within the respondent cohort nearly 40% of respondents have at least two and in some cases three devices (Table 6.8). "*Don't know yet …but I think I'm getting an iPad*" (Respondent 12). "*I use the computer that is in my office at home, it's really just*

a study. If I go away, then I rely on the tablet" (Respondent 15). Other results indicate that some older people may be acquiring different devices as part of a search for a system that is easier to use, and less difficult to understand. "*My machine is a desk top – a Hewlett Packard - and I use Vista.*" (Respondent 21).

Table 6.9 Device and System confusion.

Device and System confusion	
Understanding of computers, tablets and mobile devices	25% of respondents stated no knowledge or understanding of how to use or set up their devices, 75% of respondents indicated system and device knowledge
Easier to use	33% of respondents stated they used Apple products because they were less complicated and easier to use, 67% Made no claim to ease of use
Incorrect or mistaken understandings	28% of respondents made statements of understanding about their devices that were flawed, 72% of respondents made statements consistent with ownership of devices

Several respondents (25%) stated having little understanding of the products that they use (Table 6.9). "*No idea… it's a computer. My daughter does the technical stuff*". (Respondent 5). They appear driven by products that have market appeal *"I think I'm getting an iPad".* (Respondent 12). *It's a Microsoft program on the home computer… I just open Outlook and go from there*". (Respondent 16).

6.3.5 Management of Emails

Participants were asked how they went about storing, organising, deleting or otherwise treating their email communications (Table 6.10). All respondents were asked the question "*Do you ever delete emails, or do you place them in folders? Or do you have lots of old emails that you can still access?"*. This question revealed a broad range of responses. Some participants cited that they never deleted anything whilst others cited that they deleted all emails. "*I just open them (emails). I don't delete and I don't store in folders. They just stay where they are*". (Respondent 1). Similarly, some participants described storage in email "folders", whilst other respondents cited the practice of cleanouts where all emails from the past would be deleted. "*I haven't deleted any emails yet. I just open them. I know how to save them as unread, so if there are ones that I want to find again I click them so that they save as unread emails for later*". (Respondent 4). Other respondents cited a more organised approach: *"Yes I delete emails, and yes I store emails in folders, lots of old emails, in folders".* (Respondent 13).

176

Table 6.10 Management of Emails.

Management of Emails	
Leaving emails	47% of respondents had no intention of refiling, or categorising their email correspondence. 53% of respondents indicated sorting email in some format.
Aiming to keep all emails	64% of respondents stated that they kept all email correspondence and did not delete emails, 36% of respondents cited the practice of deleting some email correspondence
Left Unopened	14% of respondents left emails unopened, 86% of respondents either opened all emails or opened some emails and deleted some emails
Storage and Management Advice	24% stated that they relied on the advice of others about whether to store, file, or delete emails from their system, 76% of respondents stated that they knew how to manage their email-correspondence independently of others

"I never delete anything. I have two folders that I transfer the emails to. One is called 'Done' and the other is called 'VIP'. Actually - I had to get rid of a whole stack of emails about 6 months ago, the computer sent me a message saying that I had run out of storage space on my drive. So I did delete a lot of old emails. Actually it didn't make much difference, and then after I spoke to the man at the computer shop he suggested I delete some photos… and I tried that, and it worked, because the message went away after that". (Respondent 7). With the exception of freeing up space on their systems, most participants did not articulate any reasoning in support of managing their emails.

Almost half of the respondents (47%) cited that they neither "stored" nor "deleted" emails (Table 6.10). Instead they would open them, and leave them in the backlog of emails. Some respondents described this list as a sub group into which emails were deliberately shifted, whilst other respondents described leaving the emails as unopened and then noting them as the emails that remained in bold font on their queue of emails (Table 6.10). A broad range of practices indicates different ways in which emails are managed. Some respondents cited hundreds of emails kept for many years but never accessed. Others cited management practices that demonstrated a low understanding of the storage and management issues from email communication. "*I spend a lot of time sorting through my emails these days. I have a set of folders where I allocate emails. Some are for friends, some are for my seniors club, and some are for my utilities. I DO delete emails as well… usually those that are trying to sell me something, as well as the emails that are making ridiculous offers and promises*". (Respondent 8).

From those who retain large quantities of email correspondence, 24% of respondents cited advice from a friend or family member as their reasoning behind their email management practices (Table 6.10). *"Once I've opened the emails we transfer them to a separate spot on the computer called 'keep'. My friend makes me choose the ones that I want to keep, and then we delete the others. Then we go to the deleted file and delete them again. I think that's what we do. I remember my friend saying that we had to delete them a second time to make sure that they are gone"* (Respondent 20).

"I delete a lot of emails, and my son tells me that I should be clearing your deleted box out, so I suppose I do have them stored in a file that's marked delete. Because my son said that even though I've deleted them, they are still there. I keep many emails, particularly ones that have got photographs in them" (Respondent 21).

Some respondents saw their email systems as repositories for important documents or pieces of valuable information. "*I keep all of my emails… even the rude ones (laughs). You never know when you'll need them. Actually it comes in handy. I forgot the address of a friend of mine from the UK, and I looked up her old message and got it from that… easy*". (Respondent 11). For some respondents, their email management centred on saving the email into an unread status. *"I haven't deleted any emails yet. I just open them all. I know how to save them as unread, so if there are ones that I want to find again I click them so that they save as unread emails for later"* (Respondent 4).

The responses to email management revealed that only 11% of respondents showed either knowledge of or an inclination for the practice of allocating and managing their communications within a set of files. In its place were a set of practices and suggestions that demonstrated minimal understanding of a management approach to emails. Of the total respondents there were 26% who admitted the wholesale deletion of all emails. "*Yes I delete emails all the time If they are spam, or unwanted adverts then I just delete them. And I have lots of old emails, but I keep them in separate folders under the names of my different friends.*" (Respondent 19).

6.3.6 Issues with Password Protection

This section asked whether older people use passwords to securely access their devices. Participants were asked "Do you use a password to access your computer?" Participants were also asked "Do you have more than one password, and if so, how do you remember them?" (See Table 6.11) The responses demonstrated that a large percentage of participants (37%) allowed others to use their computer and gave them password access. "*I have a couple of passwords and a couple of PIN numbers. I write them in a book, which only I know where it's kept*". (Respondent 18).

Table 6.11 Password Practices

Password Practices	
Password access given to others	37% of respondents gave password access to devices, applications, and email correspondence to people other than family members, 63% of respondents stated that they did not give password access to any people outside the immediate family
Access to family	53% of respondents share their password with someone else (eg: husband, wife, son, daughter), 47% of respondents did not share access with any family member
Password written on paper	67% of respondents kept their password written somewhere on paper, 95% of respondents made mention of a password or a written reminder for a password, 33% of respondents stated that they did not leave a password written on paper.
General Password access on devices	72% of respondents do not have a password protecting their computer or mobile device, 28% of respondents had a password or pin number for their device

The question revealed that less than half of the respondents had discrete password protection for their computer or device. Some participants were candid in their acknowledgement of low level password security. "*I only have the one password. I use it several times. I keep it written on a piece of paper... and that stays out of sight under the keyboard*". (Respondent 4). Participants demonstrated less concern for a digital password than for other forms of physical security such as keeping their house locked. "*Nope, don't need one. It's just me at home, who am I trying to prevent from using my computer?*" (Respondent 7). More than half of the participants (53%) indicated that they shared their password with another family member (a husband, wife, son, or daughter). "*No – err – yes – my daughter and her husband, both know the password for the computer*". (Respondent 10). "*Yes – my son has access to everything. I rely on him for setting new things up on my computer, so it makes sense that he can get into the machine too*". Respondent 17) (Table 6.11). A small number of participants (9%) also shared their email access with a friend. "*Just my friend Jane... she helped me to get started*". (Respondent 20).

The findings revealed that 72% of the respondents did not actively use a password to access their computer, laptop, tablet, or mobile phone. Of these participants, some cited their physical protection as a sufficient barrier in preventing access by others to their systems. "*It's just me at home… who am I trying to prevent?"* (Respondent 7).

6.3.7 Issues with Remembering Passwords

This section asked people who use passwords whether they have multiple passwords, and how they remembered different passwords. This revealed that 67% of respondents kept their passwords written on a piece of paper (Table 6.12). The use of written reminders was prominent throughout 95% of the interviews. In some cases, that paper is hidden, or kept in a purse. "*Yes, and I know you will be disappointed, but I keep them all written down on a piece of paper. I know it's dangerous, and someone could get access to all my computer things, but I really can't remember the passowrds, and I've got quite a few".* (Respondent 19). *"I keep it written on a piece of paper that stays out of sight under the keyboard".* (Respondent 4). "*I have a few of them and I can never remember all of the numbers. I keep then written down on paper so that I can remember"* (Respondent 7). One participant acknowledged that their password was stored in written form in an industrial safe for protection. "*Yes I have a very dangerous system of writing them down and putting them in a safe". (*Respondent 16). Many of the respondents acknowledged that the storage of passwords in simple written form is potentially unsafe. "*I have a few passwords. I keep them on the back of a business card and I keep it in my wallet"* (Respondent 22). Several participants explained that they know that the practice is unsafe, yet they continue to follow the practice anyway (Table 6.12). One respondent claimed to be able to remember their password. Two respondents explained that they stored their passwords on a digital storage device that was itself protected by a password.

Table 6.12 Remembering Passwords

Remembering Passwords	
Acknowledgement of unsafe practices	78% of respondents acknowledged that they knew their system for remembering their passwords was unsafe, 22% of respondents stated assuredness of their ability to recall their passwords from memory.
Password written on paper	67% of respondents kept their password written somewhere on paper, 95% of respondents made mention of a password or a written reminder for a password, 33% of respondents stated that they did not keep their password written on paper.
Multiple Passwords similarly derived	58% of respondents admitted that they had multiple passwords that are very similar, but have one or two characters that are different, 42% stated that their choice of password was very strong and would be difficult to break

Some participants revealed that whilst they had multiple passwords, they were essentially derivative versions of the same core password. "*I've got four passwords that I use, but actually they are really just the same password made slightly differently to the previous password. I have one that is the same as my main password, but it also has numbers after the words. So I really only have one password to remember. If I use the wrong one, I just try the next variation. I have them written on a card that I keep in my wallet… (Don't tell anybody will you?)*". (Respondent 11). Several respondents relied on changing numbers in a password to create a new password, but would keep the word for their password. "*I have some passwords for things such as Banking, Facebook, Ebay, and Hotmail. They are essentially all based upon the same password, but with a few different added numbers and passwords. That way I can remember that the password is one of four possibilities.*" (Respondent 8).

Additional responses included difficulties in remembering PIN numbers for Automatic Teller Machines (ATMs) and also for electronic Funds Transfer at Point of Sale (EFTPOS) transactions. "*I have other passwords for other parts. I keep them on the notes section of my iPad. I don't think that I could possibly remember them all*" (Respondent 25). 38% of all respondents disclosed that they knew the practice was inappropriate or unsafe. Older people demonstrated through their practices that they are not content to rely on their memories for the recall of passwords on demand. Instead they are reverting to physical security as a means of protecting their assets. "*I have a few passwords that I keep on a piece of paper and I leave it under the keyboard. I don't try and remember them.*" (Respondent 23).

6.3.8 Retained reliance upon written (postal) correspondence

This section asked whether people retained a preference for written correspondence (eg: letters) by means of the postal system, or whether they held a preference for online communication systems (eg: email). The query aimed to differentiate frequency of communications, destinations and to ascertain what categories of correspondence were engaged. For example, if written correspondence was a retained practice, did the correspondence take the form of bill paying, or was it more squarely aimed at personal correspondence such as written letters?

The question revealed that 68% of the respondents retained the use of written correspondence in preference to email (Table 6.18). *"Yes I send letters in the normal way. It's not just me that doesn't know how to send emails (haha)".* (Respondent 12). *"Oh yes – I send letters all the time".* (Respondent 9). In the remaining 32% of respondents there was a shared division of correspondence between emails and written correspondence. *"I don't send letters anymore... does anyone? I send Christmas cards, that's all. Mostly I just use the telephone"* (Respondent 7). *"I send forms like my insurance renewal off. Anything that needs a signature. Most of my regular bills – I just pay them at the Post. Umm – I send out Christmas Cards each year, at the Post – but I forgot this year, and then it was too late, so I sent a couple of friends a Christmas email. I don't think they thought much of the idea. Neither replied! (Laughs).* (Respondent 11).

The question indicated that there are large numbers of older people who have not accepted email as their principle method of communication (Table 6.13). Some respondents (21%) who notionally reject email cited it as a less useful correspondence platform than the postal system. *"Yes – I write letters. Not so many as before, but it's still a good way to keep in touch. You probably think I'm silly, but I find that it's quicker to write a letter that it is to send an email. And it's cheaper too. I've spent a lot of money on computer protection programs just so that my email is secure... the funny thing is that I'm still not certain that I'm any better off".* (Respondent 4).

Table 6.13 Reliance on Postal Communication

Reliance on Postal Communication	
Preference on Postal communication over email.	67% of respondents indicated that Postal Mail was their preferred method of communicating over email, 33% of respondents stated either online usage or preference for an online system of communication.
Postal communications seen as safer	39% of respondents stated that Postal Mail was either safer or that is was more secure than using email, 61% of respondents stated that they felt email communications was a safe method.
Email less personal than postal mail	32% of respondents indicated that email was either less personal, or deemed inferior to communication by means of postal mail, 68% of respondents stated that email and online correspondence was adequate for each person.

This section showed disapproval for email over postal mail (Table 6.13). Respondents gave answers that showed discontent towards email as a replacement for postal correspondence. "*I think it's a bit impersonal if I send an email*". (Respondent 21). Some respondents saw emails as more practical than emails. "*I send my grandchildren birthday cards… it's a good way to conceal a $20 note inside the card inside an envelope, and it's easier than trying to buy a present these days*". (Respondent 19).

6.3.9   Frequency and Usage of Web Access

This section asked respondents to indicate how often they used the Internet and looked at the World Wide Web. The question revealed a polarisation of two views towards usage of the Internet. There were 53% of respondents who showed enthusiasm in detailing the ways that they surfed the Internet on a daily basis (Table 6.14). "*Whenever I have a spare moment… I love to surf the Internet*" (Respondent 1). The remaining 47% were far less interested in internet usage in their explanations about surfing the Internet. "*Hardly ever. If someone sends me an email … say for a trip or for a club excursion, then I'll check out the event and click on the blue words… you know … the web connection line … and have a look. If I can see some photos of where we are going, I'm more likely to fork out the money and go on the trip*". (Respondent 7).

Table 6.14 Web Usage

Web Usage	
Enthusiasm towards regular daily internet usage	53% of respondents indicated a desire to regularly access the Internet on a daily or frequent basis, 47% of respondents stated that they used the Internet only occasionally or on the basis of a specific need.

This question indicated two distinct groups within the study cohort. There were those who regularly used the Internet, and those who indicated a lack of need to use it. *"I don't use the Internet very much…hardly ever. Only if there is a specific reason or an occasion where I feel I want to get a different perspective about something, like if I'm travelling".* (Respondent 15).

6.3.10 Access by others to devices and respondent access to the devices of others

This section aims to determine what issues may restrict or may encourage older people to interact more across different systems and different hardware. Internet usage when examined only based on interaction in one's own home is an incomplete and therefore potentially inaccurate indicator of usage. Access to other devices may reveal additional information about trusted or non-trusted usage and behaviour. The findings from this section indicated that 94% of respondents interviewed were either unwilling or unhappy at the prospect of using another person's devices. "*No I'm scared of other devices, especially tablets because I don't know what to do*". (Respondent 6).

Table 6.15 Access to devices owned by others

Access to devices owned by others	
Accessing someone else's device	94% of respondents were uncomfortable to access and use devices belonging to others, 32% of respondents stated the need to use someone else's machine for work, or in a public space such as a library
Someone else accessing an older person's device	27% of respondents were prepared to allow access to family or friends, 0% of respondents were prepared to allow non-family, non-friends access and usage of their device.

Cases where older people extended the access to, and usage of, their own hardware for the benefit of others was deemed by respondents as an appropriate usage. Members of family and friends were granted access by 27% of respondents. The majority of older people stated that others should not have access to their systems. "*Nobody uses my laptop… though my husband sometimes uses my tablet* ". (Respondent 13). "*No never, I don't!...no"* (Respondent 16). "*No one uses my computer… however I have used my daughter's computer on two occasions".* (Respondent 14).

Many older people indicated disquiet towards the notion of extending their interactions and the activities of others into their own hardware and the hardware of others. Respondents were asked about the circumstances when they allowed others to use their hardware (Table 6.15). *"Only my grandchildren, when they come over I don't really get to use it (the iPad) anymore"*. (Respondent 2). "*I have a computer and a tablet and a smartphone… and nobody else uses it apart from my son and my daughter-in-law. I use other people's computers if I help with relief teaching, that's all"*. (Respondent 21). "*No it's just me. Oh and my son has helped me to set up email and so on, but that's all"*. (Respondent 11). Information stored on their own machines was a minor theme with 77% of respondents citing usage restrictions on others was restricted to specific friends and family. "*Only my two friends, they are my teachers really, they are helping me to use the computer. I don't use anyone else's though, except at the public library. I have used that a couple of times too"*. (Respondent 4).

6.3.11 Knowledge about smartphone technology

This section looked at specific knowledge about smartphone technology. Participants were asked to explain the difference between smartphones and other mobile phones. The findings for this section indicated that the majority of respondents were not well acquainted with smartphones and mobile phone technology. The results show that 68% of older people had little or no knowledge about smartphones (Table 6.16).

Table 6.16 Smart Phone Technology

Smartphone technology	
Basic understanding of the application or internet capabilities of a "smartphone"	68% of respondents had little or no understanding of what constituted a smart phone, 76% of respondents did not know that it could connect with internet

Most of these respondents were unable to articulate meaningful descriptions about the key differences between mobile phones and smart phones (Table 6.16). Most respondents did not understand the implications of a phone that could harness the Internet, and reverted to making comparisons on the basis of phone calls. *"I don't really know much about smart phones, I think they can go online for messages too can't they, but whenever I've checked them they are really pricey. I've got my phone at home and that's enough for me"*. (Respondent 7). Some respondents had very little understanding of the key differences. *"I suppose being smart it's more of a fashion accessory… ha ha ha. No sorry, I don't know what's so smart about them at all"*. (Respondent 2).

Beyond the phone comparisons, some respondents understood some of the fundamental differences. *"A smartphone is newer. It's one of the expensive mobile phones that also has a computer in it. You can use it to read emails and you can play games on it".* (Respondent 8).

6.3.12 Banking Practices and the problem of statements

This section asked respondents about aspects of online banking. The findings showed that the majority (72%) of respondents were dependent upon banking statements that were delivered by postal mail (Table 6.17).

Table 6.17 Banking and Statements

Banking and Statements	
Reliance on paper statements	72% of respondents relied upon the statements that come in the postal mail, 16% of respondents look at statements on line by printing them out onto paper, 28% of respondents relied on online statements, or ATM receipts
Trust in paper statements	23% of respondents preferred paper statements because they could be trusted more than the figures that could be seen online, 8% of respondents said that staying online doing banking for too long is risky, so they would opt to print out a statement and go offline, 77% of respondents stated that paper statements and online statements held the same trust value.

In terms of financial systems and the shift to online processes, most older people remain confident of the existing physical systems of banking. *"I rely on printed bank statements. I don't trust the iPad for banking, and it's far too complex anyway. Instead, I just go to the bank and withdraw money when I need it. If I'm unsure about the balance, the teller at the bank will print me a sheet with my balance and a copy of recent transactions so that I can work out how much money I have".* (Respondent 2). Some respondents showed concern at the additional burden of online banking, either in terms of their understanding of how to perform online tasks, or in terms of banking without the help of others. *"I haven't got to any of that stuff for the computer yet. I am not ready to do money things because I really have no idea about how my computer works. I get a statement in the mail though, and the girls at my bank all know me, so if I ever have a problem, they are really helpful. They let me know if I am getting close to my limit on my credit card"* (Respondent 4). Other respondents were confident in using online banking to find out their bank balance. *"I occasionally do it online… on the tablet"* (Respondent 13).

For most interview respondents their banking habits are disconnected from, or only partially connected to, online banking. *"I do have a banking program, but I don't use it very often. My son set it up, but I find it too complicated, and I would rather just look at the statements that come in the mail".* (Respondent 17). Several respondents spoke of not needing to do anything online. *"I check it at the bank. I still have a passbook and the teller keeps it up to date for me. I also get statements in the mail. So I don't need the computer to do anything".* (Respondent 20).

Those who engage more closely with online banking are capable of describing a process in which their banking is perceived to be dependent upon online structures that may or may not appear flexible. *"I wait for the bank to send me an email telling me that my statement is ready. I click on the link and it changes the webpage to the bank banking pages. Then I have to fill out my account name and password. Actually it has two passwords, so it's really safe, although I can't remember the passwords, so I guess that's a problem. Once I'm in to the account, I can print off the statement or save it onto my computer. I usually do that, and then check my statement in my own time. I don't like the idea of staying online with the bank for too long because I don't want to get hacked".* (Respondent 8).

6.3.13 Online Banking versus ATM versus Teller banking

This section asked respondents to indicate their money-transfer banking practices where the choice existed between banking online, using an Automatic Teller Machine (ATM), or conducting their business through a physical interaction with a teller at a bank, as per Table 6.18.

Table 6.18 Online, ATM, and Face to Face banking.

Online, ATM, and Face to Face banking	
Preference form banking	68% of respondents preferred to make a transaction face to face with a person in a bank, 12% of respondents stated that they felt they were either slowing the bank inside or slowing down the queue at an ATM, 32% of respondents preferred to use an online system to perform their banking transactions
Trust in ATM banking	28% of respondents were not prepared to use an ATM at night or where the ATM machine was located externally after business hours, 18% of respondents prefer to go inside a bank because they are known to staff inside the bank, 72% of respondents used an ATM as and when required
Accessibility issues	38% of respondents cited difficulty with accessing the ATM due to screen size and vision-related accessibility, 13% of respondents stated the need for assistance in banking (across all formats, 62% of respondents stated that they were able to use ATM machines.

42% of respondents cited that they did not trust some ATM environments. In some cases, they preferred to use an ATM inside a busy shopping centre, or otherwise use the ATM machine located inside a bank branch. 28% refused to use an ATM at night or where the machine was located on the outside of a shopping centre before or after normal trading hours. 68% of respondents preferred to make a transaction with a person (ie inside a bank) rather than use an ATM or via online banking (Table 6.18). *"If I use an ATM machine, but only the ones at the bank, just inside the glass doors."* (Respondent 14) Accessibility issues are associated with the use of ATMs. 38% of respondents cited difficulty with the size of the screen at their ATM and the need to either be with someone else to assist using the ATM, or to go into the bank in person. *"I have used the ATM a couple of times, but it's too hard to read. The screen is tiny and I just can't read the instructions. I go inside my bank most times, but I try and go when they're not too busy and I don't hold anybody up in the queue".* (Respondent 4). Some respondents stated that they trusted handing their money to a person more than trusting it to a machine. *"I don't trust the machine (ATM). If I'm depositing money – I like to give it to someone in person."* (Respondent 8)

6.3.14   Trust and Usage of Social Media

This section asked respondents about their preferred social media platforms and asked what participants used, or were intending to use. Respondents were asked about their knowledge of social media and their trust and usage of social media. Nearly half of all respondents (48%) stated that they had no intention of trusting or using a social media platform.   A further 17% of respondents had considered using social media, but were hesitant because they had heard of issues from others. 71% of the respondents cited a safety or security concern in being involved in social media. 97% of all respondents referred to Facebook. 93% of respondents showed some level of concern for safety if using Facebook (Table 6.20). Some respondents referred to social media usage that was more purpose-driven, such as the need to buy or sell things through social media sales platforms such as EBay and Gumtree. Others stated their distrust for social media, making connections between the advertising columns in Facebook and attempts to lure them into buying things online (Table 6.21).

Table 6.19 Social Media Intended Usage.

Social Media Intended Usage	
Intention or aspiration to use a social media platform.	1% of respondents cited an intention to try a social media platform at some stage 48% of respondents stated that they had no intention to use a social media platform in any way 26% of respondents indicated current usage 17% of respondents had thought about trying social media but were hesitant because they had received some kind of warning or advice not to use.

Almost half of all respondents negated the intention to use a social media platform (Table 6.19). *"I don't trust any of that nonsense. It's just a way for them to find your secrets out isn't it? They lure you with the idea that you can see photos of your family and friends, whilst they suck you dry for information and sell it to others … at least that's what I think."* (Respondent 2). Others spoke of their concerns at using social media based on the advice of others: *"None so far. I have talked about facebooking a lot but there seem to be quite a few of my friendswho think its too dangerous, so I'm not in a real hurry"* (Respondent 4).

Table 6.20 Social Media Trust and Usage.

Social Media Trust and Usage	
Safety or security	71% of respondents cited either a safety or a security concern with being involved with social media, 22% of respondents stated that they felt safer with face to face or telephone conversations than using social media, 29% of respondents indicated they used social media regularly
Trust perceptions of Facebook	93% of respondents stated concern and apprehension over the use of Facebook 97% of respondents referred to Facebook specifically when discussing social media 7% of respondents stated that they used and trusted Facebook.

The results showed a high level of concern for the use of social media and in particular Facebook. Whilst 29% of respondents stated that they were users of social media, 71% cited safety or security concerns in engaging with social media (Table 6.20). *"I'm not joining Facebook because it's too dangerous – and I'll have my identity stolen from me."* (Respondent 5). Some respondents went further, saying that the preferred to communicate in face to face ways rather than by using social media. *"I don't use any of that stuff. I keep getting asked to use Facebook, but I prefer to talk to people face to face … or just use the phone."* (Respondent 7)

Table 6.21 Social Media Purpose-related Sales Usage Vs Targeted advertising.

Purpose-related Sales Usage	
Issues where social media used to buy or sell, versus issues where a social media platform was advertising to sell to the user	29% of respondents cited they would use social media selling platforms such as Gumtree and Ebay, 62% of respondents stated that they wanted to ignore the lure of social media, 9% of respondents indicated they had no need to look at social media

Some respondents were involved because of a sense of purpose or need. *"I have a Facebook account and an EBay account, oh and Gumtree."* (Respondent 8). Whilst some respondents viewed Facebook as an appropriate environment to swap goods and information, other respondents saw a separation between social media and the goodsbased platforms such as eBay and Gumtree *"Everybody wants me to join Facebook. A load of nonsense if you ask me. The only one I look at is EBay, but I've never actually bought anything from it."* (Respondent 11). Some cited that they had no need for social media at all. *"No – I don't want to be on any of those, it doesn't appeal, and I don't have the need. I don't want millions of people who don't know me trying to become my friend, I'm too old for that sort of stuff"* (Respondent 14).

6.3.15   Perceptions from Jargon

This section looked at the level of familiarity that older people had with terms that are referred to in the context of ICT information security. Respondents were asked about their understanding of two terms that emerged from the literature review as being of significance and influence in the security, usage, and trust of online banking systems. By looking at the terms "Cookies" and "Trojans" the responses indicated that older people had a limited range of understandings about terms that are in common usage and which are often referred to in the context of trust and security in ICT (Table 6.22).

Table 6.22 Knowledge and Opinions of Technical Jargon.

Knowledge & Opinions of Technical Jargon	
Knowledge and Understanding of Cookies	74% of respondents said they didn't know what the term meant, 18% of respondents stated that they weren't sure what a cookie was, but that they felt it was something to be concerned about, 8% of respondents said that they knew what cookies did.
Knowledge and Understanding of Trojans	42% of respondents stated that they didn't know what the term "Trojan" meant and that they didn't know what effect it could have on banking, 19% of respondents stated that they felt it strange that they should be expected to know about something called a Trojan, 58% of respondents were unsure of how Trojans impacted online banking, but knew enough to understand that Trojans were unsafe.

The responses showed both ignorance and misunderstanding towards terms and jargon that are in common usage in ICT context where trusted usage might include basic technical knowledge. With reference to the term "Cookies" 74% of respondents explained that they did not know what the term meant. 18% of respondents said that they weren't sure what they were but that they felt that they were something to be wary of (Table 6.22). Several respondents made inferences based on pop-up requests that they had seen on their devices. *"I know they're bad on my iPad because I often get asked with a box that says: 'Çan we use Cookies?'... So that can't be good."* (Respondent 2). Others made suppositions based upon their cited limited understanding that they might be dangerous because there were options that allowed the user to delete cookies. *"I don't fully understand them – I've heard of them – and I know on my tablet there's a thing where you can delete cookies ... which I do. Because I think that they show where you've been."* (Respondent 13). Some respondents saw them as a requirement that meant some applications needed the user to have cookies. *"I know for some things you have to have a cookie – but I sort of feel vaguely uneasy about using them – I think I've heard that we can identify information about me. It's my own ignorance."* (Respondent 14). Several respondents were wary that cookies would enable some form of tracking and identification. *"I know about these – because they sometimes come as a question asking if I want to accept cookies – especially on the iPad. It's so that they can track where you look on the Internet isn't it? I don't have any secrets, it's not as if I look at anything naughty (laughs)."* (Respondent 19)

Respondents had varying degrees of understanding about the term "Trojans" (Table 6.22). 58% of respondents were unsure of exactly how a Trojan might make their online banking practice unsafe, but felt that they knew that a Trojan was representative of something unsafe. 42% of respondents were ignorant of the term Trojan" and of any effect that a Trojan could have upon secure online banking (Table 6.22). *"I don't know much about Trojans – but I think they're bad too".* (Respondent 2). Several respondents took guesses as to what was meant by the term "Trojans". *"Nothing ... I don't know... though I'm guessing from the name that it's something bad?"* (Respondent H8). Many of the responses showed some portion of understanding in combination with statements of uncertainty. *"I don't know; I'm grasping at straws a bit – are Trojans like infections? – No I don't know."* (Respondent 15). Some

respondents associated usage of an Apple product as protection against Trojans. *"Yes – they are dangerous aren't they? I know that if I get an anti-virus message about a Trojan that it's a serious thing. That's why we have the Apple computer because it's much safer."* (Respondent 19).

6.3.16 Perceptions about online deception.

Respondents were asked if they thought that they had ever been deceived online. The responses were varied. They showed that there were a variety of different perceptions about online deception. Responses were more consistent in their identification of friends who they knew had been deceived online. Responses indicated that attempts and deception is widespread. 75% of respondents indicated an agreement or statement about some form of online deception that either they or friends that they knew had experienced. 68% of respondents stated that they knew of a friend who had been scammed or deceived online (Table 6.23).

Table 6.23 Perceptions of Online Deception.

Perceptions of Online Deception	
Older persons knowledge of a friend who had been deceived online	68% of respondents indicated that they knew of a friend who had either been deceived or scammed in some form of online activity, 32% of respondents indicated they knew of no one who had been deceived online.
Recognised an attempt at online deception	75% of respondents stated that they had been able to recognise online attempts in emails to deceive them, 25% of respondents had no perceived experience of an attempt to deceive by means of email.

Many respondents spoke of what they had heard from others as part of their knowledge about online deception experiences. *"I don't think so. My friend has – she said she ended up getting a computer technician who needed three weeks to get rid of something that infected her computer. That's why I'm just going slowly, slowly for the moment. I don't want to make a mistake and then end up paying for it later."* (Respondent 20). Other respondents recalled specific events that they could recall personally. *"Yes I think I have been scammed before ... it was an email to day that there was a parcel available at the post office – and I had to print out a receipt so that I could collect it – but I had to verify my information – so I sent it off – and then afterwards I found that there wasn't any such parcel – I had*

192

just handed over my personal account information. I had to change my account at the bank." (Respondent 21). Some respondents recalled emails and phone calls that appeared to the respondents as attempts to deceive them. *"We've had loads of those scam emails. We've had ones from Nigeria, and several about winning lotteries. They are so easy to tell as fake. Oh and we get the Microsoft phone (call) ... just about every week. I happily tell them that I have a Mac and then they hang up, it's the best thing to say. Mind you – there is always another person ringing up again."* (Respondent 19). Other respondents stated that they were confident that they were unlikely to befall an online deception. *"No – I've heard of others – but I don't get many emails so I reckon I'm fairly safe."* (Respondent 18).

Several respondents (13%) revealed that they could relate an experience an incident where they had been deceived and had required the assistance of an IT technician or a repair service centre. Some reported a financial incident whereby part of the incident required them to change banking account numbers or credit cards in order to prevent further losses (Table 6.29).

Table 6.24 Experienced Online Deception.

Experienced Online Deception	
Older persons experience of an online deception.	13% of respondents indicated that they had experienced an online deception in the form of something that required intervention and repair by an IT technician or repair centre, 87% of respondents had no reportable experience of an online deception.

The majority of respondents did not indicate a personal experience of online deception, whilst 13% of respondents cited an experience that required some form of repair or intervention in order to return to their previous online system. In some instances respondents cited that they were safer because they used Apple products. *"I did have one time when I got an email saying that my storage was full (I do keep quite a few emails), and I foolishly clicked on the line that they said to click in order to fix the problem. Then after I filled in my password I realised that I could no longer access my emails. Someone told me that I had been hacked. Anyway after I went to the computer shop, they helped me get my account back, we had to reset my password quite a few times – just to throw the hackers off the scent I suppose ... anyway it all worked out in the end. That's why I bought an Apple computer. It's so much safer now, and I never get that kind of email anymore."* (Respondent 8). In an isolated instance one of the respondents acknowledged falling victim to a financial deception involving a sizeable sum of

money. *"Um – pause – I have actually. I got an email from a man who said he was collecting money for a wonderful cause that helped African boys to receive enough money to go to school. Well it turned out to be a scam, but not before I sent him quite a bit of money. It was nearly $15,000 in the end. I just delete most of my emails now. It was a very nasty experience."* (Respondent 2)

6.4 Interviews Part Three – Trust and Money

The third section of interview questions focused on issues of trust and money. The questions also explored issues about the trust of online information. Respondents were asked a series of questions designed to elicit responses that differentiated between the trust held in people and organisations, and the trust held in online systems and computer programs. Questions were also asked about trust in smartphones and their associated apps. Respondents were asked questions that aimed to establish the ways and means by which participants reconcile ideas about technology trust.

There were five questions that were put to the participants. The first question asked "Why do you/don't you trust computers? The second question asked participants "do you know enough about computers to feel comfortable using them for finance and banking? The third question asked about Facebook usage and whether you would trust someone else to set up a Facebook account on your computer or device? The fourth question asked people to consider engaging with an online banking program where you were required to trust the bank even before they had made a transaction. The last question asked about the trust people have in a smartphone to store personal information. All five questions provided a challenge to participants by asking them to consider situations where the security of participant assets was potentially at risk.

6.4.1 Sending money and trusting issues

This section asked respondents about why they did, or did not, trust computers. Respondents had a variety of reasons in support of their answers (Table 6.25). Some respondents pointed out that in instances where they had no choice but to use an online system, it was difficult to trust a system because there was no choice about whether the system could be swapped for something alternate.

Table 6.25 Trust issues with money transactions

Trust Issues with money transactions	
Trust in using a computer for money transactions	56% of respondents stated that online banking is not a trustworthy system for completing money transactions, 44% of respondents indicated that online banking could be trusted if undertaken by a person of sufficient training and ability
Trust in one's own skill and capability whilst using a computer for money transactions	44% of respondents stated that the main problem area in trusting online banking was their own capability, 56% of respondents indicated that they would trust themselves to perform online transactions based upon sufficient training and ability
Trust for passive (online bank statement viewing) versus active (making an online transaction) interaction	46% of respondents stated that they operated within a limited set of activities, where they were prepared to view an online statement or bank balance, but were not prepared to actively make an online banking transaction, 54% of respondents stated that once trained they would not only view statements, but would undertake banking transactions
Trust from forced and imposed usage of online banking	24% of respondents stated that they were unhappy that they now had to use online banking, and that previous methods of banking in face to face was a more trusted system to use, 76% of respondents acknowledged that online banking was unlikely to disappear in the near future
Trust in online banking versus emails	72% of respondents stated that online banking had a much higher level of risk than other computer activities such as emails and internet browsing, 28% of respondents stated the need to exercise caution regarding the security of all online activities.
Trust in emails and offers relating to online banking	38% of respondents stated that offers to use apps for banking, and emails that requested users to update their information portrayed online banking as untrustworthy, 62% stated that email spam was an everyday part of online communication

Some respondents (56%) said that they did not trust online banking as a system for the purpose of making financial transactions. The remainder of the respondents characterised the trust in online banking by referring to having the necessary competency to undertake online banking (Table 6.25). Several respondents stated the need for significant training before they would trust using an online system for financial transactions. *"I don't really trust computers because they seem to be more complicated than I can understand. I just don't get them. I mean I have tried to do things to change my settings, but it just gets too hard. There seem to be an endless supply of options, and I'm never really sure whether I'm making the right choice.To tell you the truth, they make me realise that I'm a bit of a dummy"* (Respondent 2). Some respondents explained their lack of trust in terms of trusting themselves to use an "online-only" system, where none of the other supporting options (such as postal statements and bank branches) were available. *"It's not just a trust issue – it's also about choice. Take banking for example. I can go to the bank, I can use an ATM, or I can do banking from my PC. But if you force me to only use the online system – then I'm hesitant to trust it."* (Respondent 1)

A significant number of respondents (44%) stated that they held concerns about their own capability to securely undertake financial transactions using online banking. Responses noted caution about the combination of both inadequate self-capability and hesitation to trust in a system that allowed people of low capability to use it (Table 6.25). In these examples respondents are citing their inability to trust a system because of a lack of information about online banking as well as a lack of computer background and skill on their own part. *"There seem to be an endless supply of options – and I'm never really sure whether I'm making the right choice. To tell the truth – they make me realise that I'm a bit of a dummy."* (Respondent 2). Some respondents saw their own lack of information as the reasoning behind not trusting computers; they focussed on their likelihood of losing money by using computers. *"It would just be too dangerous for me; I'm too old, I don't know all the tricks and traps, and I'd end up losing money. So I don't trust computers for that."* (Respondent 4).

The respondents were split in regard to what kind of banking transactions that they would undertake safely and securely. 46% of respondents indicated a limited acceptance of using online banking, citing their preference to passively use online banking to see statements and balances, whilst 56% of respondents stated that after sufficient training and skills, they would undertake regular online banking in both a passive and an active transactional sense. (Table 6.25). Some respondents explained the difference in terms of either banking using a variety of bank options to banking using only online banking. These comments regarded the options that were "online only" as financially insecure. *"You hear so many stories about how unsafe it all is. Every time we go to the seniors' club – that's the main topic of discussion. It's almost a competition to see who has the scariest story. None of us trust computers. But we know that we are increasingly getting told that we have to use them. That doesn't make me trust them any more I've got to tell you. The money side of things is the most worrying. I just can't afford to lose the money I've got. If I start to trust computers and lose it – what will I do, then?"* (Respondent 5).

28% of the respondents stated that using a computer was unsafe, and that there was a high probability of being taken advantage of by either a system, a criminal, or an organisation. Some of these were prepared to look at emails and internet, but not to attempt online banking (24%), whilst others

(17%) were prepared to passively look at online statements but were not prepared to actively undertake transactions using online banking (Table 6.25). *"Sometimes I get these emails sent to me – they ask me to try things – and that scares me – so I just ignore them. But it worries me. I don't trust the emails at all. So I try not to read too much of it – I just delete the emails as quickly as I can so that the viruses can't get in to my computer. If I'm not sure then I turn it off at the wall so that they can't get started, you know – they can't get a foothold inside the computer. I don't know if they're real or not – but I just don't want to take a chance."* (Respondent 6)

72% of the respondents regarded online banking as having a much higher level of risk than other computer activities such as emails and internet browsing. Many respondents combined their online banking risk aversions with hesitations about their own online skill capabilities (Table 6.25). *"I don't use my computer as much as others ... I'm sure. I really missed the boat when there was an opportunity to learn about computing. So I don't do anything outside of what is comfortable. I can read emails and I know how to get on to Google, so I can check things out if I need to. It's not that I don't trust computers, but I know that if I tried to use the computer for other things I would be trying things that might put me at risk, so I just don't do anything that isn't about emails really."* (Respondent 7). Some of these respondents cited a partial trust in computing, stating a trust in the reliability for the computer to turn on or to operate normally. However they also cited a lack of trust in the computer system not to be infected with malware (Table 6.25). *"I trust them for simple things such as sending and receiving emails. But when you look at some of the social media programs – they are just asking for trouble. It's no wonder many people fall victim to scams. It's full of strangers making claims and offers. It's not an honest environment. So I don't trust it. As for the machine – it's like any other – I trust it to turn on when I switch it on – but then there are so many stories about viruses that I think – how can I trust a computer. I'm not very skilled at computing – so please don't ask me to identify a virus – I wouldn't know where to start. So in that context – no I don't trust computers."* (Respondent 9)

There were 32% of respondents who spoke in terms of their own capabilities, citing that the main area of trust was in trusting themselves or their own actions rather than the trust associated with the computer itself. 12% of Respondents (overall) spoke about fault and blame in assigning the problem of trust to their own abilities and behaviours (Table 6.25).

"It's not that I don't trust computers, but I guess I don't trust myself ... I mean I don't really need to trust computers. I'm quite happy as I am, I would like to buy things from eBay, but it's no problem, and my son said he'd get anything for me if I wanted a specific thing online. I'm lucky like that – so I don't have to trust in computers because I've got other people. And they're a lot better at using computers than me that for sure (laughs)." (Respondent J11)

Responses to the questions about trust in computers attracted many detailed replies. Participants gave responses that tied multiple trust-related elements into reasoning about the various elements of trust in terms of hardware, software, personal capabilities, and financial risk. Included in these responses were a range of answers that stated that the effort required to maintain the required skills and knowledge was increasing. 13% of responses stated that they felt they would never catch up to the required level of skill and knowledge to be able to trust in the usage of ICTs for online banking. *"I don't particularly like doing anything involving money. I'm not really "anti" the digital world and using computers, but on the face of it I think it's far more-risky, and it's a lot harder to form an understanding. So it's partly that I'm not ready to do something, like banking online, but I think it's more because there are so many security issues that relate to computing. I hate passwords – they are the bane of my life – but I don't want criminals and hackers to enter my computer. I don't want to have someone steal my identity, and I don't want to get scammed. I constantly get reminders that I am at risk, and the whole thing makes me realise that I really can't trust computers in general. Yes, it's partly my fault – because I don't know enough – but it seems as if there is always something new to learn, or a new app to download, or something. It's never ending. It's not like learning to drive. When I went for my licence) many years ago of course) I had to sit for the test and pass the driving exam. After that I was fine. But when I'm using the computer – it seems that I am constantly having to learn something new – or to update*

something. I get the sense that I will never reach the point when I will be sufficiently knowledgeable that I'll be able to use the computer with any real confidence. (Respondent 17)

24% of respondents stated that they were unhappy that they were forced to use a computer where it had replaced a physical human system (such as bank tellers or postal statements) which had, in their opinion, being running to a satisfactory level. These respondents were explaining that there were previous (non-computer) systems and arrangements with which respondents were quite happy with, and for which the need to change to a com`puter-related course of action implied some level of distrust (Table 6.25). *"I don't think I should have to do this. Let me say this – Do I trust strangers that come to my door or approach me in the street? No. Do I trust computers that send me messages and offers and requests that I haven't asked for? No. The whole idea is that computers are strangers to me – or if you like computer machines bring strange offers into my life, and I totally reject that idea. I don't want it, I didn't ask for it, - it shouldn't be something that takes up much of my thinking. So I don't trust computers because much of the interaction – the emails – the Facebook – the offers off taking up a financial banking app – they are all about pretending to help me – when in fact they are all about helping some other group or business. There are the email scams – some might be from individuals and others from organised criminals – but then there is Facebook that gives or sells my details to businesses, and then there are banks who want me to work for them. They want me to download my statement, print it out on my printer, with my paper, my ink, and my time, and they want me to take the risk of knowing my password, paying for anti-virus to keep my computer secure, and essentially doing a whole range of things that the bank already did when they sent me a statement in the mail. I don't trust computers – and I don't trust people who are trying to make me use them more and more."* (Respondent R18).

6.4.2   Comfort levels when using computers for Finance and Banking

In this section, respondents were asked if their level of comfort extended to using computers to undertake financial applications and online banking. Of the respondents 61% stated that they were not comfortable to do their own online banking. Some respondents (12%) stated that they felt that they were uncomfortable because they felt they were forced to learn about online banking (Table 6.26).

Respondents made a clear distinction between the access of a balance using an online banking app, and the more active use of setting up a computer for the purpose of sending money, paying bills, and using a computer for online banking transactions. In some instances respondents equated comfort with usage. Other respondents described their comfort in terms of whether their usage was voluntary or mandatory. Some respondents drew a connection between comfort and security. Other respondents connected comfort to the idea of skill and capability. Some respondents described their comfort in terms of the level of complexity or simplicity attached to what they were doing.

Table 6.26 Comfort levels in online banking.

Comfort levels in Online Banking	
Discomfort to conduct one's own online banking	61% of respondents stated that they were not comfortable to do their own online banking, 32% of respondents stated no uneasiness at online banking, 7% of respondents stated that they felt at ease using online banking
Forced to learn	12% of respondents stated that they were forced to learn about online banking despite the desire to return to more comfortable systems such as face to face branch banking, 37% of respondents stated that online banking was being imposed upon them with very little real choice to avoid it, 51% of respondents stated that they understood the need to offer online banking as an option
Simplicity of Online Banking	32% of respondents stated that they did use online banking on a regular basis and that the process was simple 7% said that they felt slightly uneasy about doing online banking 47% of respondents said no to online banking 14% stated they definitely wouldn't use online banking.

The majority of respondents stated that they were uncomfortable with online banking. *"I'm not really comfortable – no. There's just too much at risk. I'm not trained in online computer finance. That's what the tellers at the banks are for."* (Respondent 21). Some respondents stated that they felt forced to take part in online banking and mentioned that this was a factor in their discomfort in using online banking over other methods. *"I do use a computer for banking, but I don't trust myself all of the time, and I do feel that it's quite a lonely thing to learn… to use computers, I'm not sure that I'd describe it as 'comfortable' but necessary. I don't really have much of a choice"* (Respondent 8). Other respondents cited that they were comfortable with using online banking. *"Well yes – as I said – although with some help from my husband (He worked for a finance company and he knows his way around all of our systems."* (Respondent 19).

6.4.3 The Setup and Adoption of Social Media such as Facebook

In this section respondents were asked to comment on their social media usage and in particular their association with Facebook. Each respondent was asked to comment on whether they set up their own Facebook account, or whether they had assistance from someone else. Respondents were asked to explain whether they would trust someone else to set up a social media platform for them and under what conditions would they trust someone else to use their computer or mobile device (Table 6.27).

Table 6.27 Setup and adoption of social media

Setup and adoption of Social Media	
Independence and assistance to set up Facebook	62% of respondents stated that they relied upon assistance, 6% of respondents installed and setup Facebook without the assistance of a friend / family member, 32% of respondents stated that they would not use Facebook

Many respondents related their decision to either setup or not setup Facebook in terms of a reliance upon someone else. Facebook usage was connected with the approval or non-approval of another, rather than on their own judgement or independently formed opinion. The reliance upon someone else was in some cases connected to a decision not to set up Facebook or social media. In other cases the reliance on someone else showed an extended trust in that other person to the point where they would set up a Facebook account (Table 6.27). *"I would get my son to set it up, I trust him, or perhaps someone from the seniors club that I trust."* (Respondent 21). Some respondents explained that their use and installation of Facebook was conditional upon support from others. *"Yes we have Facebook. My son set it up and showed us how to set the privacy settings so that only our friends and family could see what we put on Facebook. I know I'm old, but my family is making sure that I stay very tech savvy."* (Respondent 19). Other respondents stated that they felt that they were coerced, but remained unwilling to take part in using Facebook. *"No my daughter tried to set it up for me – but we haven't used it. I don't trust it – and I don't want to give up my details and secrets to the rest of the world. I'm a private person and I'd like to keep it that way."* (Respondent 5)

Many respondents referred to the need to have someone else assist to set up Facebook because they did not have sufficient skills to set it up on their own. Other respondents described the need for

someone else to assist in terms of their trust in that person, and their decision to use (or not use) Facebook on the basis of the usage of that other person. Several respondents made a connection with the expertise or IT related background of another person as an important part of the decision to proceed with the installation and setup of Facebook.

Only 6% of respondents stated that they would install and set up Facebook on their own and without assistance from someone else. Some respondents spoke of installing Facebook in terms of the Faceboook program being installed onto their computer. Other respondents described the installation of Facebook as a more involved process that included not just the installation of a program, but also the set-up of internal settings and features (such as privacy settings, and security settings) so that the program was prepared and able to withstand security-related interactions of concern and incidents perceived as risky .*"Never again, I had it, it was stupid, and then I was bombarded with people trying to sell something. There were endless emails about things others had done – and I just couldn't keep up. I mean – if I want some company – I'm better of going to the (seniors) Club."* (Respondent 2)

6.4.4   First time trusted usage of online banking

In this section, respondents were asked about using a banking application for the first time on a mobile device. They were specifically asked what would give them sufficient trust to use an online banking application (Table 6.28). Several respondents described the need for IT training. Some respondents were specific in describing the need for either a sustained period of training, or specifically face to face training, or sufficient training to provide a high level of proficiency. The answers from respondents in some cases stated that long periods of training, "months", would not be enough time for them to gain sufficient proficiency to be able to use an online banking application for the first time. Others stated that there was no level of training that would be sufficient to enable them to develop enough trust in an online banking system (Table 6.29).

Table 6.28 First time trust of online banking.

First Time Trust of Online Banking	
No trust in first attempt at online banking	67% of respondents stated that they would not trust their first attempt at online banking, 33% of respondents stated that they would need substantial training or an assistant in person to undertake online banking on their first attempt.

The majority of respondents stated that they were unlikely to trust their fiorst attempt at online banking. Responses included the need for extensive training and assistance, and many responses indicated the need for human interaction as part of a person's first attempt at online banking. *"I wouldn't ever use such an application – not unless it came with a full time computer technician and someone on hand to constantly explain everything... and I don't mean a help desk or a call centre either. No. I would need someone physically in the room with me – showing me – slowly – and teaching me what to do. And they would need to be patient – because I'm not the kind of person who gets things the first time. You would need to show me several times for me to understand."* (Respondent 2)

Table 6.29 Sufficient Training for First Time Trusted Use

Sufficient Training for First Time Trusted Use	
The requirement to receive enough training so that a person would engage in using an online banking system for the first time.	36% of respondents stated that they would require significant and / or specific training so that they could use an online banking system for the first time, 57% of respondents stated that they could not imagine a scenario with enough training to make them trust the first time usage of an online banking application, 7% of respondents stated that they would trust and use an online banking application

The majority of respondents (67%) stated that they would not have any trust in their first attempt at online banking (Table 6.28). 26% of respondents stated that they would need specific training before attempting to use online banking for the first time. Respondents commented on the need for training, and expressed their needs with a variety of stipulations: that some would need extensive or lengthy training, whilst some stated the need for face to face training and side by side assistance. The answers regarding trusted use drew out strong responses that placed a high emphasis on ICT expertise and capability when connected with personal online control of a financial application.

Many respondents cited their need for training as part of the necessary steps towards trusting the use of online banking. *"Lots and lots of training. I just think it's an unnecessary risk ... and I don't see the need to take risks like that. Right now, my money sits in bank accounts, and I can get at it when I need to. I would need to feel proficient at using my computer to start using anything online for money.*

I think I'm much safer letting the experts do online things to my money. That's what the bank does best ... not me." (Respondent 7). For some respondents there was no sufficient amount of training that would allow for a respondent to trust the use of online banking. *"I wouldn't try this – even if I had many months of training. The bottom line is that there are some things that you shouldn't put at risk – and at my age – my money and my savings are not worth putting at risk."* (Respondent 9)

6.4.5   Trusted Information on Smartphones

Respondents were asked in this section to explain their trust in their smartphones. Respondents explained about whether they trusted their smartphone as a place where personal information was collated. 23% of respondents stated that they trusted their smartphones, and that they used them for keeping contact information and for internet access. 63% of respondents stated that they either did not know or did not understand how a smartphone kept trusted information. 13% of respondents stated that they could not store trusted information on a smartphone because of accessibility reasons such as the inability to read small print, and the ability to use the phone securely or properly (Table 6.30).

Table 6.30 Trusted information on smartphones

Trusted information on smartphones	
Trusted use of smartphones for stored information	23% of respondents stated that they trusted their smartphones
Lack of understanding of how a smartphone worked	63% of respondents stated that they either didn't know or didn't understand how a smartphone could store trusted information.
Accessibility Issues	14% of respondents stated that they could not store trusted information on a smartphone because they were unable to see or navigate the smartphone in a manner that was safe or secure.

Many respondents demonstrated limited understanding about smartphones and their capabilities. Some respondents cited that they had limited trust of smartphones, and did not see the need for trusting smartphones to store information. *"No I don't trust smartphones to store anything. I don't have one, don't intend to have one, ... I can't even read the numbers on the phone anyway, so it's useless to me, You'd need a phone with big numbers like my home phone. I don't think they've made that model yet have they?"* (Respondent 7). Other respondents cited the burden of using a smartphone when they were still in the process of learning to trust other technology devices such as desktop computers, tablets and

other mobile devices. *"No – my son says they are very insecure. So I have resisted the urge to buy one. ...It's just another thing to master and that makes me realise that I'll never know enough to be secure. I'm still getting my head around the computer at home."* (Respondent 17).

6.5   Interviews Part Four – Decisions of Trust, Acceptance or Rejection

The fourth section of interview questions looked at the issues of trust in greater depth. Respondents were asked to discuss technology trust in terms of risk. Additionally, they were asked about their perceptions of confidentiality and online systems. In particular, the respondents were asked about instances where they trusted other humans, advice from friends, and a range of aspects pertaining to online banking.

6.5.1   Trust in sending money, and using someone else's computer

In this section the question of sending money is used to get respondents to consider their specific trust (or lack of it) in regards to the challenge of sending money. By asking a question that specifically relates to a trust function involving a financial transaction, respondents gave experience-based answers to questions of online trust (Table 6.31). The act of asking respondents to consider trust as connected to a device or a system assists to delineate between the trust that people have in hardware and software and the trust that people have other people.

Table 6.31 Trust in sending money: using someone else's computer.

Trust in sending money; using someone else's computer	
Rejection of the idea to use someone else's computer to send money	92% of respondents stated that they would not use someone else's computer to send money.
Risk in using someone else's computer, and the preference to pay at a bank	33% of respondents stated that they felt that the task of using someone else's computer was too risky, and they would prefer to pay somebody at a bank to make the transfer.
Liability for loss or damage.	29% of respondents stated that they did not want to be held liable in the event that money was lost or misdirected.
Preference for using the bank	69% of respondents stated that they would make an attempt to use a bank rather than using someone else's computer for the purpose of sending money

The majority of respondents were opposed to juisng another person's computer to send money. 69% of respondents stated that they preferred to use a bank as a trusted system than by doing the transfer themselves using someone else's equipment and system. *"I have sent money before. But I prefer to get a bank to transfer the money rather than to do it myself - typically because if I'm sending money somewhere it must be really important – or a really large sum of money – and I don't trust myself not to stuff it up."* (Respondent 1). 33% of respondents were so opposed to using seome else's compuer that they cited a preference to pay a bank employee to handle the transfer of funds. *"Well I have already had a bad experience – so I have zero trust. I wouldn't use my computer or anyone else's for that matter. If I need to send money anywhere – and I don't think I ever will again – I will do it at the bank, face to face, in front of someone who gets paid to know how to send money."* (Respondent 2)

Respondents showed reluctance to use another person's computer for the purpose of sending money. 92% of respondents stated that they would not use someone else's machine for sending money via online banking. Two respondents stated confidence in sending money under such conditions and were only prepared to do this because the machine was operated by a person known to them and who was working in finance and who understood the need for a secure system for online money transfers (Table 6.31).

33% of respondents were specific about the risk in using someone else's computer. They stated that they would proper to pay money at a bank than to undertake a task that involved trusting someone else's personal machine. 29% of respondents spoke of concerns that they had for their personal liability in the event that the transaction was improperly done, or that money was lost (Table 6.31).

Most respondents described the idea of using someone else's computer for a financial transaction in negative terms. In some cases their concern was connected to their own inabilities. Some respondents were concerned that even though they might be able to use their own computer, the use of someone else's computer would be more difficult, more risky (in terms of their technical mastery of the computer) and more likely to incur greater vulnerabilities. Other respondents described their uncertainty about the possibility of someone else's computer being a safety risk in terms of a machine that could be compromised, or where the user might be able to access and interfere with someone's account at a later stage. Many respondents (69%) stated a preference for using a bank rather than someone else's

computer. *"Assuming I had the ability (which I don't) and the desire (which I don't) to do this – the main problem would be that of security and safety. How would I know if the other person's computer was safe to use? I can barely find my way around my own computer – but asking me to somehow understand someone else's computer is terribly chancy. And then even if I could do this – how would I know if they had the right virus software? How would I know if the machine kept my password or any account information? It would be hard for me to trust someone else's computer. Really hard."* (Respondent 5).

8% of respondents spoke of trust in using a machine that belonged to an authority rather than an individual. 4% of respondents spoke of trust in sending money as long as it involved using an Apple Mac. 17% of respondents said that they would only send money from someone else's machine in an emergency. This would not constitute a trusted transaction, but instead would represent a forced transaction (Table 6.32).

Table 6.32. Authority and Mandated actions.

Authority and Mandated Actions	
The Authority of the Bank	39% of respondents stated that they regarded the Bank as the appropriate authority to undertake bank transfers, with greater experience and greater powers
Liability for loss or damage.	17% of respondents stated that they would only use someone else's machine in an emergency, where they had no choice but were forced to engage in online banking
Brand reliance and confidence	4% of respondents stated that the activity could be trusted as long as the machine being used was an Apple Mac computer.

Respondents stated that transfers carried out by the bank rather than by the respondent on their home computer had greater trust, and also had a higher probability of success. Respondents made comparisons between the authority that was retain by a bank, as a collective of people working under a trusted system that was continually used, and the lack of authority held by an individual handling one-off transactions with little authority. *"It doesn't matter whether it's my computer or someone else's. Anything like that, I just go to the bank"* (Respondent 7). Banks were regarded by respondents as the appropriate place to go to undertake money transfers. *"I'd like to think that I could do something like*

send a large amount of money to my brother for instance. But if I think about it, I'd probably rush down to the bank and make sure that it went through properly" (Respondent 8). *"I have had to send money to the UK recently actually – and I just went down to he bank. They handled it all. Again – I'm just not that good at computers – so I don't trust myself yet"* (Respondent 11).

Many respondents stated that they would only engage in online banking if they were required to do so. Respondents stated concerns at making a mistake in transferring money. *"I don't trust myself not to stuff it up"* (Respondent 1). Respondents made comparisons between the risks of doing a bank transfer themselves and the expectation that getting someone from the bank to tranmsfer the money had a significantly reduced likelihood of financial loss. In the case of a bank mistake, respondents held the expectation that any loss would be made good by the bank, whereas any loss derived from their own actions doing online banking would result in a personal financial los to the respondent. *"I will always go to the bank … first and foremost – because I trust the people at the bank to send the money and to do the job of securing the money from my account to somewhere else. I am less inclined to do the job myself – because there is such a different level of knowledge and security for me. It's not just knowledge – it's that I'm fairly certain that the level of sophistication at the bank in their computer systems is a darn sight more advanced than in my own home. I couldn't hope to compete on that level. I also don't want to do the job of a teller. I'm not interested in getting a job at a bank. I want the bank to do the banking work – like sending money for me. As for the idea of using someone else's computer, all I can say is that there would need to be an almighty urgency for me to do that. I would not trust someone else's computer (how could I possibly know whether it was secure? Even if I knew the person – I couldn't tell you how secure they were – or how knowledgeable they were about computing."* (Respondent 17).

Some respondents spoke of past experiences that had taken away their trust in online banking. *"Well I have already had a bad experience – so I have zero trust. I wouldn't use my computer or anyone else's for that matter. If I need to send money somewhere – and I don't think I ever will again – I will do it at a bank – face toi face – in front of someone who gets paid to know how to send money"* (Respondent 2).

Some respondents expressed confidence in transferring money, and some stated that their trust was conditional on a trusted brand. *"I'm confident that we can send money from our computer. We do this a fair bit. I've never tried to do it from someone else's computer though, I think it would need to be the same as my own. I mean it would need to be an Apple computer or it wouldn't work anyway, but I'd probably hope it was a Macbook. If I think about it, it should be fine, but I don't think I'd rush off in a hurry to do that. I like the security of our own home"* (Respondent 19).

6.5.2 Using one's own hardware for online banking

In this section respondents were asked to explain their perceptions of risk in using their own computer or device for online banking transactions. This question requires respondents to focus on the risks of undertaking online banking from a personal perspective. Rather than general answers to questions about risk, this section specifically aims to draw out issues that relate to an individual on a personal level (Table 6.33).

Table 6.33. Risk in using one's own hardware for online banking.

Risk in using one's own hardware for online banking	
Lack of immediate and physical bank support	26% of respondents stated that they were concerned at the risk of conducting online banking where they did not have instant, direct, and face to face access to bank support
Risk of shared unsecured information through	39% of respondents stated that they were concerned at the potential risk of identity and account information being shared with criminals and hackers.
Comparative risk compared to transactions conducted physically in a bank.	23% of respondents stated that the practice of online banking on their own computer was less safe than physically attending a bank.
Cost outweighed by risks	13% of respondents stated that the better option would be to use a physical bank, even if that usage required additional transactional costs.

Respondents identified a number of risks associated with using one's own hardware for the purpose of online internet banking. One of the main issues identified is the solitude and isolation associated with online transactions where there is "no second chance". 26% of respondents stated that they were concerned at the risk of conducting online banking themselves in situations where there is no "hands on" physical bank support (Table 6.33).

Other responses identified that online banking is targeted by criminals who use malware such as key-logger programs (through Trojans) to record and transmit keystrokes that identify account details, passwords, and a range of other personal information. 39% of respondents stated that online banking

carried a potential risk of identity and account information being shared with criminals and hackers (Table 6.33). *"There is a modicum of risk. You need to make sure that you know what you are doing. – but also need to make sure that your computer is safe, is password protected, has antivirus that is up to date, and functioning. I have an idea of what to do now, but when I first started I was a mess. I made a few mistakes – and the bank didn't pay for any of them."* (Respondent 1).

23% of respondents mentioned that online banking was less safe than going to a physical bank and asking the bank to do the banking based on customer requests. 13% of respondents stated that online banking included a high level of worry and stress that the transaction or personal information would be adversely interfered with. Similarly, 13% of respondents stated that the better option would be to use a bank to undertake transactions, irrespective of the cost issues (Table 6.33). *"For me the risk would be incredibly high. I struggle to keep up with the statements that the bank mails to me, so I don't think trying to take it all on myself is wise. I often wonder why the bank thinks we all want to do their job for them. I reckon you'd have to be bonkers to do online banking. It's risky, at my age, there are no second chances, and it means trying something that I'm not good at. On top of that, it means using a computer amongst online thieves and bandits. It's obvious from the news that online banking cannot be trusted, and it's really only for nerdy types who understand the gobbledegook in the computer."* (Respondent 4).

6.5.3   What would make online banking a more trusted option?

Respondents were asked to describe what would make using online banking a trusted option. This section aimed to require respondents to focus on the solutions to the challenges of trusting online banking rather than the problems associated with trusting online banking. By focusing on solutions the responses would potentially differ from other questions where the inherent risk aversion to possible transactional losses might provide a different set of perceptions about trust and imposed online banking (Table 6.34).

Table 6.34 Making online banking more trusted for older people

Making online banking more trusted for older people	
Training that was significant	63% of respondents stated that they would like to see training that was significant, mentioning elements such as face to face delivery, large portions of time, and specific training centred on secure online banking transactions
Large amounts of time spent on training	47% of respondents stated that they wanted to see opportunities for large amounts of time spent on training in online banking for older people.
Comparative risk compared to transactions conducted physically in a bank.	17% of respondents stated that there was a need for high quality training in the form of specific training and at high levels such as a university level degree course.

Responses suggested different options for training, with some asking for large amounts of time on training, whilst others made mention of specific training such as attending university to undertake a degree in computing. 63% of respondents stated that significant training would assist in improving levels of trust towards online banking. *"Years of training, and the support of someone with IT Training 24 hours a day."* (Respondent 1). Many of the respondents stated the need for on demand assistance, citing the need for a real person to assist them as and when that assistance was required. *"Someone on hand at all times. Whenever I've tried online banking, I'll get to a point where there is a choice of options – and I won't be sure. But it's not as if I can turn to someone in the middle of the process and ask – what do I do now?"* (Respondent 17).

47% stated that there should be large amounts of time allocated towards the training of older people for online banking. 17% of respondents suggested the need for high quality training in the form of specific course or even university degree studies (Table 6.34). Whilst many responses cited the need for training, 63% of responses re-iterated that a preferred option was not to undertake online banking but instead to have someone at a bank perform their banking tasks for them. *"A bank employee doing the work would be a start. Seriously though there isn't any reason to use my home computer for this. It is not secure for several reasons. I'm not very savvy with computing. Banks are. I can't spot viruses and worms. Banks can. I am retired and don't want to work. Banks still want my money so they can work for it. It's not very hard to see why I don't want to do online banking."* (Respondent 9).

6.5.4 Confidence in the security of email.

Respondents were asked whether they felt their emails were secure, and if they felt other people could access them. This question aimed to gather information about how older people regarded their

email correspondence as a trusted form of communication. By asking about the confidence in the security of their email, it helped to establish whether respondents were more trusting of face to face and postal mail where some of the necessary security components involved in online banking necessitated a level of confidence in the secure use of email.

Table 6.35 Confidence in the security of email.

Confidence in the security of email	
Belief that criminals and hackers can see email correspondence with ease	32% of respondents stated that they thought criminals and hackers had the skill and the intention to see the email correspondence of individuals with relative ease.
Uncertainty about security of emails	53% of respondents expressed some uncertainty and insecurity about how they could judge the security or trustworthiness of their email communication.

32% of respondents stated that they felt that criminals and hackers were able to access emails with ease, and that emails were not a secure method of communication compared to postal mail and face to face communication. *"I know there are plenty of computer experts who can get to me, to my money, and to my emails. So I don't think emails are very safe."* (Respondent 2). 53% of respondents cited some form of uncertainty in the ability to judge whether their email communication was secure, trusted, or able to be accessed (Table 6.35).

6.5.5 Preparedness for third party set up of online banking

In this section respondents were asked whether they would allow someone else to install an online banking program on a machine of theirs.

Table 6.36 Preparedness to have online banking set up and installed by a third party.

Preparedness to have online banking set up and installed by a third party	
Resistance in the face of offers	78% of respondents agreed that they had received offers to help set up online banking but had refused the offer of any third party individuals to assist them. 22% of respondents stated they had not received an offer.
Offers from individual family members and friends	47% of respondents stated that they had received an offer from either an individual family member or from a friend to set up online banking
Reluctance to share financial information	13% of respondents stated that they refused to accept assistance on the grounds that they had no desire to share financial information or system access with other individuals.

Respondents gave answers based upon install by others nominating whether the person that was known to them was a relative, or a friend, or an acquaintance (Table 6.36). This section aimed to find

out how readily older people would accept the assistance of other parties when setting up and installing online banking systems that would then be used by the respondents.

78% of respondents had directly received offers of help to set up online banking but had refused the offer of a third party individual to assist them. *"My daughter and her husband offered to set it up – but in the end we decided not to do it because it was just too complicated – and she can't just fly from the UK every time something goes wrong."* (Respondent 10) 47% of respondents had received an offer from either an individual family member or from a friend to set up online banking. 13% of respondents stated that they refused to accept assistance because they were reluctant to share financial information, or access to it, with other individuals. *"I've had many offers to set up this or that. I refuse them all."* (Respondent R18). This included family and friends (Table 6.36).

6.5.6 Trust in Unsolicited Telephone Contact

In this section, respondents were asked to comment on how they handled telephone calls from people claiming to be from an authority such a Bank. This question aimed to determine whether older people would receive telephone calls and would accept the calls as legitimate even though their credentials were not confirmed. The question was also expected to reveal the behaviour of older people in terms of what action they would take when an unsolicited call was made to offer assistance with online banking.

Table 6.37 Trust in unsolicited telephone contact

Trust in unsolicited telephone contact	
Acceptance of unsolicited contact	8% of respondents stated that if they received a call from the bank they would accept it and treat the caller as a trusted source regarding bank issues.
Referral back to the Bank	42% of respondents stated if they get a call from the bank, they would not trust the call, but instead would refer back to their local bank to ascertain whether the phone call was legitimate in its origin.
Rejection of unsolicited contact	84% of respondents stated that they rejected the legitimacy of phone contact from someone claiming to be from a bank.

The direct acceptance by respondents of calls as legitimate was low. 8% of respondents said that they would treat the caller as a trusted source regarding bank issues. *"Well I suppose as long as I know it's my bank – then I'll trust them. It's tricky though isn't it – I mean they ask for my date of birth and what was my mother's maiden name and that sort of information … so that they know they are talking to the real me. But how do I ask them back to see if they are the real bank? It's doesn't seem fair does it?"* (Respondent 2).

42% of respondents stated that if they receive a call from someone stating that they were from their bank, they would not accept the call as legitimate, but instead would refer back to the bank to ascertain whether his phone call was legitimate in its origin. *"I'd get their details and tell them I'd call them back - then I'd check with the bank to see of someone from there had rung me."* (Respondent 13). Overall, 84% of respondents stated that they would reject a call from a bank if it were unsolicited (Table 6.37).

6.5.7 Confirming personal details over the phone

In this section, respondents were asked whether they were prepared to give personal details over the phone, when asked by a caller saying they were from a bank (Table 6.38).

Table 6.38 Confirmation of personal details on phone calls.

Confirmation of personal details on phone calls	
Admission to giving information to unverified callers	77% of respondents stated that when asked on the telephone, they had given their personal information to the caller, even though they were not sure whether the call was a legitimate, legal call, 23% of respondents said that they would not give out their information over a phone call.
Imposition and lack of choice	26% of respondents stated that they felt they didn't really have a choice, but rather that there was an urgency to give over personal information so that the rest of the call could proceed.
Refusal to submit personal information to caller	8% of respondents stated that they refused to give personal and private information over the phone, regardless of who the caller said they were.

Respondents were asked to indicate whether they would trust a situation involving a call that could not proceed until the caller had received personal details. This question aimed to determine whether older people placed a value on their personal details enough to question the need to divulge sensitive and personal information over the phone when it not clear that the call was legitimate in nature.

Many of the respondents admitted that when called and asked to verify their details they had done so without confirming the origin or intention of the caller. 77% of respondents gave an admission of having given information to a caller without attempting to confirm the origin or intention of the

caller. *"It has happened to me – the person calls and says that it's a personal banking matterand then asks for all sorts of personal information like my date of birth and address, yet I really don't know if it is in fact the bank or simply someone pretending to be from the bank. I end up giving the details every time, but I know that I shouldn't"* (Respondent 19).

26% of respondents stated that they gave information because they felt that they had little or no choice. Respondents indicated that they were prepared to give personal information to the caller so that the call could proceed and the issue could be dealt with directly (Table 6.38). 8% of respondents refused to give the caller any personal information over the phone. *"Yes – I've done this – I'm sorry – I know its stupid – I didn't have a choice."* (Respondent 19). Instead they either referred the call to their branch, or otherwise ignored the phone call in preference to some other form of contact (Table 6.38). *"I'd be uneasy – and I think I would simply revert to going directly into the branch. I had a call from the bank when my Husband died… I nearly hung up when I heard the Indian accent – because I thought it was going to be one of those calls."* (Respondent 14).

6.5.8 Trust in Recommendations of Peers and the uptake of Facebook

In this section respondents were asked to comment on how they reacted to peer recommendations such as being asked to join and use Facebook. The question is posed that there is an invitation to join Facebook by a peer for the purpose of keeping in touch. This question aimed to capture information about older people who accept the advice of their peers, and the influence of trust in areas of uncertainty. It also looked to determine whether the uptake of an ICT innovation such as Facebook held the same level of trust as for one's trust for online banking.

Table 6.39 Peer advice and Facebook agreement.

Peer advice and Facebook agreement	
Lack of Trust in Facebook despite recommendation to join by a peer.	84% of respondents stated that when asked to join Facebook their response was an emphatic refusal, and the recommendation from a peer held little or no bearing on the decision of each respondent to join Facebook. 16% of respondents stated that they used Facebook.
Imposition and lack of choice	Of the respondents who rejected the idea of using Facebook, 13% of them stated that Facebook was both risky and insecure because it changed privacy settings without notice.

81% of respondents stated a lack of trust in Facebook. In most cases the respondents rejected the idea of joining Facebook even though the suggestion had come from a peer or friend within the community. *"Yes I have had a couple of requests already. I'm not ready yet, and as I said before I'm very cautious aboutgetting it set up properly. I don't want the identity theft to happen to me. If it all gets set up properly, then I'll probably try it, but only if it is set up properly, not by me, but by someone who I trust and who know what they're doing"* (Respondent 20).

13% of respondents who rejected the idea of usingFacebook cited that it was too risky and that it was not secure because it changed privacy settings without adequate notice (Table 6.39). *"I'm already on Facebook, but I don't trust Facebook's lack of privacy. They changed my privacy settings once before – and didn't tell me."* (Respondent H8).

6.5.9 Peer Recommendations, and the trusted uptake of Online Banking Apps

In this section respondents were asked to explain their actions following advice from friends that a particular online banking application might not be trustworthy. This question aimed to determine what level of trust was connected with online banking applications, and the level of trust from peers and friends towards online banking.

Table 6.40 Trust in Peers, Uptake of Banking Apps.

Trust in Peers, Uptake of Banking Apps	
Advice from peers in general.	87% of respondents acknowledged that the information from peers was of value, 13% of respondents gave no indication of the value of peer advice.
Importance of peer advice	39% of respondents stated that the inclusion of friends and associates as informal advisors was a useful method of getting information in an area where the usage of banking apps was uncertain.
Advice from peers about banking apps	35% of respondents stated that they valued their peers, but required independent advice as well as that of other older people regarding an important venture such as the download and usage of a banking app.

87 % of respondents acknowledged that they regarded the information and advice of other older people as valuable and trustworthy (Table 6.40). *"I rely on the experiences of my friends. We warn each other about dodgy emails and scams, as well as swapping stories about things that are dangerous, or that we have tried but have not worked out. My friends are my most trusted source of IT help."* (Respondent 8).

39% of respondents stated that the inclusion of friends and associates as informal advisors was a useful method of getting information about areas where trusted usage of banking applications was not a guaranteed outcome. *"Well I do rely on information from one friend in particular. She has had a few ups and downs – so she often tells me what to do and what not to do. I listen to ger advice, she is my computer coach"* (Respondent 20). 35% of respondents stated that they valued their peers, but also needed to obtain independent advice because the issues concerned finance and banking elements. *"I listen to my friends and I usually take their advice. But in the case of banking – and because it's about my life savings – that'll never get another chance to accumulate – I will also check with a range of other people. Whilst there are different banks, there are no many options, and any choices need to be very carefully weighed up."* (Respondent 17).

6.5.10   Summary of interviews Parts 1 - 4

The first 4 interview segments revealed a range of information that qualified the participants' ideas in relation to participant backgrounds, types of ICT usage by older people, descriptions of trust, and understanding concepts of trust. These interviews were analysed by a six step coding process outlined in the next section.

6.6   Coding for Chapter 6

The process of coding the interviews is described here. The transcripts of each interview were collated in the order in which the interview questions were asked. This was arranged so that responses could be compared, associated and linked to other responses from the same line of inquiry. The process of coding is described here in three main parts starting with the identification of codes, followed by the labelling of themes, and then the recognition of concepts (Table 6.41). All the individual characteristics, all of the codes, and all of the themes are labels that are used to recognise the most important concepts that define the results of this research.

Table 6.41 The Coding Process for this Research

The Coding Process for this Research				
Step 1	**Codes** Preliminary coded characteristics	First Impressions	Read, understand, re-read and annotate transcripts, repeat step many times.	
Step 2	**Codes** Theme descriptors for labelling categories into common themes	Patterns	Label relevant parts, germane words, phrases and sentences. Includes labelling of actions concepts, differences, opinions & processes.	
Codes are Categorised into Themes				
Step 3	**Themes** Confirm categories by assigning them to theme descriptors	Create Categories	Decide which codes are significant – create categories by aligning codes together. Codes that seem collectively important are kept.	
Step 4	**Themes** Further categorisation shows the strong themes using connections & repetitions	Label Categories	Label categories and decide which are the most relevant. Examine how they are connected to each other.	
Themes are Developed into Concepts				
Step 5	**Concepts** Labelled categories developed into ordered thematic concepts	Develop Concepts from Themes. Rank by Importance.	Determine rank, hierarchy, importance. Use a diagram or a figure to help summarise results.	
Step 6	**Concepts** Realisation of results	Present coded data in a conceptualised form as results.	Coded data written as descriptions of categories and how they are connected.	

Adapted from Lofgren, (2012) Qualitative analysis of interview data.

The first part (Step 1) involved reading and reviewing the transcripts to identify codes that are referred to as preliminary codes. In this first step codes are drawn as individual attributes from the transcripts according to five criteria:

- Things that are repeated
- Something that stood out as different from the literature
- Something that a participant specifically identifies as important
- Something that relates to something identified in a previous report or article
- Something that bears a resemblance to a theory or concept

This process resulted in a set of first impressions from which a total of 90 code criteria were identified. These 90 attributes formed the preliminary coding for the data and results (Table 6.42).

Table 6.42 Codes - Preliminary Coding (Step 1)

Capability to use email	Access to expert advice 24/7	Similar Passwords	Trust in specific Operating System	Trust and usage of ATMs
Previous Training	Low level training	Re-used Passwords	Using other people's devices	Accessibility / Vision at ATMs
Confidence in Sending Email	Frequent Usage	Admissions about passwords	Understanding of Smart phones	Resistance to the use of Social Media
Confidence in using IT	Checking Emails	Passwords on paper	Reliance on Paper Bank statements	Security Issues with Social Media
Hesitation to use email	Trust in a specific brand	Derivative Passwords	Face to Face banking preferences	Privacy issues with Social Media
Misplaced Confidence	Resentment in using own equipment	Preference towards Postal Mail rather than email	Trust in people over computers	Face to Face and Telephone rather than social media.

Brand dominance of Facebook	Low understanding of the term trojans	Choice in using ICT or face to face	Trust in online statements	Concern with Facebook advertising
Low understanding of the term "cookies".	trust concern with Facebook	Ability to recognise an online deception	Imposed usage of online banking	Greater perceived online risk
Offers to take up online banking	Doing the banks work	Social Media set up by family member	Changing privacy settings on Social Media	Received additional Facebook – related ads or (SPAM)
First Time Trust	Need for training	Trust in using smartphones	Trust information stored on a phone	Trust a smartphone as a storage device
Trusting one's self to send money online	Using someone else's computer to personally send money	Preference to physically attend a bank to transfer money	Specific need for Apple brand to transfer money	Lack of immediate (real-time) Bank support
Need for significant organised training	Confidence in secure email	Hackers	Security Scams	Online banking set up by others
Distrust in offers of banking setup by others	Online Banking Problem – don't understand choices	Distrust divulging personal info over the phone	Supplying information to others	Admission of trusting others unknown
Coercion to join Facebook	Advice from friends as a source of trust	Sensitivity to sending money in private	Preference to transact through a bank	Trust in Apple brand
Doing the teller's job for them	Trust in security of postal mail before email	Resentment at cost and complexity of own equipment	Risk of Hacking/ Theft	Perception of need for huge levels of training
Unsolicited telephone contact from bank	Trust in offers from family to set up online banking	Likelihood of hackers access without my knowledge	Bank employees have better training than customers	Face to Face delivery of training
Trust in offers to have online banking set up	Giving information out over the phone	Reluctance to share financial info with family	Forced when call was of a serious or urgent nature	Refusal to give information over the phone
Ability to distinguish legitimate calls from others regarding money	Trust in advice from peers regarding Facebook	Feeling forced to divulge information to continue a call	Trust in independent advice (non-peer, non-family, non-commercial)	Trust in advice from peers regarding online banking

In Step 2 The preliminary coding was initially categorised using five coding descriptors. These formed a set of labels that were used to characterise prominent themes from within the transcripts. These were as listed in Table 6.43. These coded segments looked for relevant words, phrases, sentences and sections

Table 6.43 Theme Descriptors (Step 2)

Actions & Activities	**Differences**	**Concepts**	**Opinions & Beliefs**	**Processes & Abilities**

The theme descriptors were derived from the main areas of the literature review. In the first instance, the literature review identified that older people took it upon themselves to take action and to

undertake activities in relation to their financial assets, the security of their assets and the use of new technologies. The Technology Acceptance literature (TAM) demonstrated that there were many variables and differences that affected the acceptance of these technologies, and that it was therefore important to examine differences as a key descriptor within the coding process.

The literature pointed to the importance of differences in terms of technology capabilities, socio economic factors, trust in people, and trust in systems. The literature also showed that older people made decisions based on conceptual understandings in relation to technology and in relation to trust. Opinions and beliefs were included as key theme descriptors because the literature demonstrated that older people held a variety of beliefs about perceptions of trust and distrust. Similarly the literature allowed the researcher to conclude that processes were very important in identifying how older people went about interacting with trust-related aspects of financial management. In combination with physical, financial, and traditional capabilities, the use of processes and abilities was prominent in terms of identifying areas where older people have been previously identified as influenced in terms of trust and decision-making. By using these five descriptors, individual phenomena could be identified and categorised so as to assist in the labelling of notable characteristics.

By using the five coding descriptors and by analysing the preliminary coding it was possible to recognise themes (Step 3). In this process coded attributes were brought together under more general categories.

Table 6.44   Themes Step 3

Activities and Actions	Concepts	Differences	Opinions and Beliefs	Processes and Abilities
Capability and Trust	Confidence in secure email	Doing the teller's job for them.	Trust in Advice from others (family, peers)	Capability to use email
Trust using other devices	First Time Trust	Brand Domination of Facebook	Distrust in offers to set up online banking	Need for significant organised training
Trust in telephone calls	Confidence in sending email	Low understanding of the term cookies	Trust in usage of ATMs	Frequent usage
Trust one's self to send money online	Confidence in using IT	Don't understand online banking choices	Trust in specific operating system	Need for training
Previous training	Misplaced confidence	Ability to distinguish legitimate calls from others in money	Hesitation to use email	Ability to recognise an online deception
Low level training	Offers to take up online banking	Low understanding of the term trojans	Trust in online statements	Social media set up by family member

Checking emails	Access to expert advice 24/7	Admissions about passwords	Trust in offers to have online banking set up	Ability to recognise an online deception
Doing the Bank's work	Sensitivity towards sending money in private	Resentment at cost and complexity of equipment	Preference towards Postal Mail rather than email	Understanding of smartphone technology
Coercion to use Facebook	Similar Passwords	Forced to divulge information to continue a call.	Resentment in using one's own equipment	Face to face delivery of training
Giving out information	Re-Used Passwords	Reliance on Paper bank statements	Specific trust concern with Facebook	
Forced use of ICT	Derivative passwords	Face to Face banking preferences	Trust in others using one's own device	
Unsolicited telephone contact from a bank	Choice in using ICT or Face to Face	Trust in people rather than computers	Advice from friends as a source of trust	
Using someone else's computer to send money	Physically attend a bank or online transfer money	Imposed usage of online banking	Trust in security of postal mail before email	
Giving information out over the phone	Sensitivity / Privacy in send ing money in private	Bank employees have better training than customers	Trust in family members to set up online banking	
Keeping passwords on paper	Reluctance to share financial information with family	Accessibility / Vision Issues at ATMs	Trust in online statements	
Social media set up by a family member	Changing privacy settings on social media	Security issues with Social Media	Perceived need for high level training	
Distrust to divulge info over the phone	Trust information stored on a phone	Privacy issues with Social Media	Hackers and futility	
Using other people's devices	Security Scams	Greater perceived online risk	Rise of Hacking and theft	
Supplying information to others	Preference to transact physically through a bank	Lack of immediate (on call) Banking support	Trust in using smartphones	
Forced to comply with info on serious or urgent matters	Trust in independent advice	Online banking set up by others	Specific need for Apple brand to transfer money	
Resistance to using online social media	Face to Face and telephone rather than Social media	Trust information stored on a phone	Likelihood of hackers access without participants knowledge	
Refusal to give info over phone	Concern with Facebook advertising	Trust in Apple brand		
		Trust in strangers		

In Step 4 the resulting set of themes form the principal categories by which the data is organised and analysed. Attributes and preliminary codes are cross referenced to other labelled themes and strong themes emerge from alongside others. The coding considers how many times different attributes re-appear in different themes, and allows these themes to emerge as the more robust parts of the coding process. It considers how many different descriptors each theme has a connection with. These strong themes provided the framework by which the data has been conceptualised so as to interpret the results of this research.

As stronger more connected themes emerged they were ordered against the main label categories (Table 6.45). These categories allowed for both general and abstract themes to be ordered and assembled. The themes were categorised under three label headers. To guide the process of categorising themes, the process of labelling used a three way ordering process of Adaption, Seeking Information, and Problem Solving (Table 6.6). This assisted the task of determining the most important themes.

Table 6.45 Themes - Strong Themes Step 4

Activities & Actions	Concepts	Differences	Opinions & Beliefs	Processes & Abilities
Successful Experiences from ICT usages	Trust in using ICTs	Accepting information storage on digital devices	Greater trust in Humans over Systems	Capabilities for Communicating using ICTs
Experiences with ICT of Limited success / failure	The need to protect money and finances	Taking over banking roles previously done by Banks	Information on paper carries highest legitimacy	Capabilities in security requiring specialised training
Interactions with those seeking to sell or deceive	The need to control Privacy, Information, and Assets	Making under-informed choices about ICT usage	Likelihood that Digital information can be altered for malevolent purposes	Training using face to face delivery
Experiences with new, different, others ICT equipment	Control Methods for ICT security	Understanding ICT-based risks and uncertainties	Information and advice of peers is highly reliable	Full / extended understanding of ICT opportunities
Actions arising from Family assistance and intervention	Reduced / Limited Face to Face experiences	Interactions with systems without people	Belief in specific Brands	Ability to recognise ICT-related deceptions
Actions requiring compliance	Mistakes, Misplaced Trust, Poor Advice		Older people more targeted more vulnerable than others	
			ICT is difficult	

The process of connecting the main themes to the labels of Adaption, Seeking Information, and Problem Solving in some instances involved overlap (Stringer, 2007; Lofgren, 2012). Some main themes would, for example, fall under both Adaption labelling and Problem Solving. Table 6.46 shows where main themes interconnect with different labels in order to further conceptualise the data. It sorts the themes from table 6.45 into groupings using the labels adaption, seeking information, problem solving.

Table 6.46 From Themes to Concepts. Step 5.

Activities & Actions	Concepts	Differences	Opinions & Beliefs	Processes & Abilities
Successful Experiences from ICT usages **PS**	Trust in using ICTs **A, PS**	Accepting information on digital devices **A**	Older people more targeted more vulnerable than others **SI, PS**	Capabilities for Communicating using ICTs **A, PS**
Experiences with ICT of Limited success / failure **PS**	The need to protect money and finances **PS**	Taking over roles previously done by Banks **A**	Information on paper carries highest legitimacy **A, SI**	Capabilities in security requiring specialised training **A, SI, PS**
Interactions with those seeking to sell or deceive **A**	The need to control Privacy, Information, & Assets **A, PS**	Making under-informed choices about ICT usage **SI, PS**	Likelihood that Digital information can be altered for malevolent purposes **SI**	Training using face to face delivery **SI**
Experiences with new, different, others ICT equipment **A**	Control Methods for ICT security **SI**	Understanding ICT-based risks and uncertainties **SI**	Information and advice of peers is highly reliable **SI**	Full / extended understanding of ICT opportunities **SI**
Actions arising from Family assistance and intervention **A, PS**	Reduced / Limited Face to Face experiences **A**	Interactions with systems without people **A, PS**	Belief in specific Brands **SI**	Ability to recognise ICT-related deceptions **SI**
Actions requiring compliance **PS**	Mistakes, Misplaced Trust, Poor Advice **A, PS**		Greater trust in Humans over Systems **A**	
			ICT is difficult **A, SI, PS**	

Key	A = Adaption	PS = Problem Solving	SI = Seeking Information

6.7 Conceptualising the Data

To conceptualise the data from the strong and emergent themes the process categorised the themes against the main criteria for Emancipatory Action research. By sorting the strongest themes into Adaptions, Problem Solving, and Seeking Information categories, the results can be interpreted in terms of emancipatory actions (Zuber-Skerritt, 2003; Baskerville and Wood-Harper 1996). This provides a clear method of interpreting the results as concepts. Table 6.47 shows what involves adaption from one thing to another, problem solving of key challenges, and identification of what parts involve the seeking of information.

Table 6.47 Conceptualising the Data. Step 6.

Adaption	Problem Solving	Seeking Information
Trust in using ICTs	Successful Experiences from ICT usages	Information on paper carries highest legitimacy
Accepting information storage on digital devices	Trust in using ICTs	Capabilities in security requiring specialised training
Greater trust in Humans over Systems	Capabilities for Communicating using ICTs	Making under-informed choices about ICT usage
Capabilities for Communicating using ICTs	Experiences with ICT of Limited success / failure	Likelihood that Digital information can be altered for malevolent purposes
Taking over banking roles previously done by Banks	The need to protect money and finances	Training using face to face delivery
Information on paper carries highest legitimacy	Capabilities in security requiring specialised training	Control Methods for ICT security
Capabilities in security requiring specialised training	The need to control Privacy, Information, & Assets	Understanding ICT-based risks and uncertainties
Interactions with those seeking to sell or deceive	Making under-informed choices about ICT usage	Information and advice of peers is highly reliable
The need to control Privacy, Information, & Assets	Actions arising from Family assistance and intervention	Full / extended understanding of ICT opportunities
Experiences with new, different, others ICT equipment	Interactions with systems without people	Belief in specific Brands
Actions arising from Family assistance and intervention	Actions requiring compliance	Ability to recognise ICT-related deceptions
Reduced / Limited Face to Face experiences	Mistakes, Misplaced Trust, Poor Advice	Older people more targeted more vulnerable than others
Interactions with systems without people	Older people more targeted more vulnerable than others	ICT is difficult
Mistakes, Misplaced Trust, Poor Advice	ICT is difficult	
ICT is difficult		

The data was then categorised to show these connected themes as concepts. These were ordered as either *adaption*, *problem solving*, or *seeking information*. Some themes fell into more than one concept grouping. In the case of themes that fell under Adaption the concepts were grouped as either a concept of trust in ICTs or as a concept of Human versus Digital trust. Themes from the Problem Solving subset fell under the sub-heading of Choice in Using ICTs. The set of themes developed under the heading of Seeking Information was centred on the concept of trusting in Information that was accessed by means of a digital system.

6.7.1 Adaption

The Concept of Trust in ICTs. This concept included the acceptance of information storage on digital devices, capabilities in using ICTs, trust in communicating using ICTs, interaction with systems, overcoming the complexities of ICTs, coping with the expectation of using new ICTs, relying on banking using ICTs, control over the privacy of digital information and assets, using ICTs to the same

professional level as paid (Bbanking) professionals. Choices in banking systems. Choice in financial systems.

The Concept of Human versus Digital trust. This concept included the cultural hesitation to trust systems above trust in people. Interactions with systems without people Mistakes, Misplaced Trust and Poor Advice. Reduced Face to face experiences, Actions from Family assistance and interventions. Reduced choice in human versus digital experiences.

6.7.2   Problem Solving

The Concept of Choice in Using ICTs. This concept includes the challenges of decision making where ICTs are involved. It involves interactions without human interaction, or reduced face to face interactions. It also includes the issue of capability, and the ability to trust one's own ICT usage in comparison to the capabilities of others. This concept includes the notion that for older people the use of ICTs in financial transactions has a level of complexity, and that older people are more targeted and more vulnerable in their ICT use than others. The Cost of using ICTs. The ability to access ICT systems and other choices for trusted financial transactions.

6.7.3   Seeking Information

The Concept of Trusting in Information via Digital means. This concept includes the challenge in understanding the accepted trust of digital information. This concept is about how older people place greater trust in paper documents than in digital on-screen information regarding. It covers the issues of learning new skills to engage in a digital environment, as well as learning how to make decisions and evaluations about risk in digital systems, as well as the risk of leaving human systems to digital ones. The concept also includes seeking information about the norms and standards of ICT usage. It examines the opportunity to choose a different system or an ICT system, but incorporates the choice with issues of accessibility, risk, and complexity. The concept goes beyond normal understanding about the usage of ICTs to include a strong focus on the security of one's digital assets and finances.

6.8   Results from the data

The analysis of the data identified and categorised a range of themes into conceptualised data. The results were analysed in terms of order to identify hierarchies. Some themes were more strongly affirmed than others, and this resulted in a greater weighting on some results than others. These themes are discussed below through the three lenses of Adaption, Seeking information, and Problem Solving.

6.8.1   Adapting to Change

In terms of adaption-based themes, the results point to five main areas. Table 6.46 showed those conceptualised main themes as connected to the idea of adaption. Some of these are sufficiently connected to form the dominant themes that underpin these results. These main areas focussed on general ICT capabilities, trust in digital information storage, perceived vulnerability to cybercrime, choices involving face to face and human exchanges, and independence to interact without the need for the assistance and intervention of others.

The results point to significant challenges in the shift from interactions with people to interactions with systems where face to face communications are removed or severely restricted. This extended to suggest that trust and acceptance of ICTs is the subject of scrutiny and comparison. The results show that there is reluctance for many older people to move away from existing systems that are not directly perceived as ICT systems, and to accept, use and trust different and novel systems that are perceived as ICT systems. This reluctance occurs across a range of transactions including the use of emails (to the exclusion of postal mail), the use of online banking (to the exclusion of postal bank statements), the use of smartphone apps (to the exclusion of face to face information), and the use of digital devices operating in 24/7 mode (instead of banking activities during Monday to Friday shopfront banking store hours). Older people cited key differences in terms of their aversion to shift away from systems that they perceived to hold human and physical contact in the form of face to face encounters, personally addressed mail, and peer to peer information exchanges.

The results show that older people view changes towards ICTs as more complex in terms of the understanding required operating different devices. In particular the shift from paper-based information (such as bank statements) to the digital storage of information from online banking applications was regarded as less secure, more complicated, more time consuming, and more expensive.

Older people believe that they are more targeted and also more vulnerable than other age cohorts. They perceive that part of their vulnerability is connected with their lack of understanding of ICT systems and processes. Many responses drew connections between limited ICT capabilities and the likelihood of financial losses. Losses were expected from cybercrime, risks from interactions with non-human systems, poor communications with non-human ICT help systems, and lack of specialist ICT training. Face to face banking experiences were seen as inherently safer and less complex. These types of interactions were also seen as more secure because the onus of the transactional part of the banking was perceived to remain with banking staff rather than with the respondents.

Several important themes had strong inter-connections. Older people regarded the physical existence of a bank as their principal means of storing money in a secure manner. A strong theme was that in combination with limited ICT knowledge and capability, the use of online banking placed financial assets at greatly increased risk of loss through two main pathways. The first was the perceived higher likelihood of loss through exposure to malware, hacking, and other forms of cyber-related deception. The second was from the perceived higher likelihood of personal mistakes and errors through reduced ICT skills, inability to trust devices, lack of access to human support (in the form of face to face or phone-based assistance), and inability to remember or access passwords in a safe and reliable manner.

Many respondents raised the question as to why they were expected to do the work of bank staff. They showed an aversion to doing online banking transactions because in combination with an increased risk of financial error, there was also an increased cost in terms of the purchase of computing equipment (desktop, laptop, table, smartphone) and the perceived need for peripheral devices such as a printer.

These challenges were further compounded by issues of trust, deception, and choice. Respondents made comparisons between face to face interactions and online or telephone interactions. They felt more secure in face to face exchanges, citing uncertainty in perceiving deception in the form of email requests, sales offers, and telephone calls. Online and telephone interactions were perceived as risky because in many occasions they were asked to divulge personal information about themselves to establish identity, in instances where they were unable to make determinations about the true intentions of the online system or telephone caller. Respondents cited that when the choice between an online and a face to face interaction was removed (or when it was highly coerced towards an online interaction), that their trust in the online transaction was diminished.

One theme that was strongly indicated was in terms of independence. Respondents indicated that in instances where they were forced or obliged to use online banking their trust was further diminished because they became dependent upon other people and other things. There were many mentions from respondents saying that they were not sufficiently trained, or that they needed assistance from others. There were mentions of the need to use other people's devices (computers and printers) because they could not afford to buy equipment. There were mentions that they could not make determinations about the security of their environment because they might not trust someone else's computer, or that they felt that someone else might then later use that computer to access money. The theme of lack of independence is connected perceptions of diminished trust, uncertainty about the security of financial transactions, and reduced ability to have control over the banking process. Many cited preference to have bank employees make transactions on their behalf as a matter of choice. Related to this theme was the absence of discussion about stopping online banking. There are no responses that condemn or refute ICT-based banking, but rather the discussions are focussed on the desire to choose between face to face banking and ICT systems.

6.8.2   Seeking Trusted Information

In terms of Seeking Information themes the results point to four main areas. Table 6.46 showed the main themes in a conceptualised form as connected to the idea of seeking information. Some of these are sufficiently connected to form the dominant themes that underpin these results. These main

areas were the ability to choose face to face delivery of information, the trusted reliance upon peer-derived information, the trust in information on certain product brands, and the need for greater information, understanding, and training to improve ICT capabilities.

In addition to the themes under heading of adaption, the data pointed to several themes relating to seeking information. Older people discussed the different ways in which they sought information relating to the safe and trusted use of ICTs. The distinction between information sought from face to face discussions and information that came from online information was a strong theme. Older people associated strongly with the idea that their local community groups and close friends were trusted sources of information. The data showed that peers from within the older community were perceived to be the most trusted sources of ICT information. Other sources of information that were strongly associated with trusted use were family and friends. Whilst some respondents associated with family members as trusted sources, there were differing expressions that suggested that family members may have reduced choices by imposing ICT usage. In these instances many of the responses associated strongly with reduced trust and acceptance.

The theme of brand trust emerged as strongly connected to ICT usage from trusted information. There was strong agreement with the perception that Apple (and Apple-related products) had systems that could be trusted. The data showed 98 specific mentions of the brand in terms of its reliability in terms of security. Comments referred to safer and more secure online transactions, safer communications, and greater detection and protection from viruses and malware. Wider comments relating to the imposed use of other's computers also associated with brands.

The themes of training and capability were prominent features of the data. The main idea centred on the need for high level training that was face to face. Discussion on training made many specific references to the human delivery of quality ICT training in preference to online training, online tutorials, and web-based help systems. The inclination towards face to face training delivery was also associated with increased perceptions of trust in the information. Online training by contrast was associated with higher likelihood of information deception. Two ideas were prominent. Online information was

sometimes regarded in terms of security dishonesty. It was also regarded as misleading in terms of perceived influence for the purpose of gaining a commercial advantage. Much of the mainstream commentary drew connections between the attempts by banks to convince people to either convert to online banking, or at least to cancel out of arrangements where bank statements were sent by postal mail.

Those seeking information about bank offers and online banking associated the commercial offers alongside ideas of misleading promises about ease of use that directed new customers to online tutorials and information portals but removed face to face information choices. These were associated with lower perceptions of trust. In other instances there was strong association with online information as complex and more difficult to understand. These comments connected with diminished trust because there was a perception that older people's capabilities in using ICT were less reliable than other younger cohorts. The theme of retaining face to face choices for training and ICT usage were much higher regarded in terms of trust and reliability. Those seeking information for the purpose of improved capabilities in terms of banking security strongly associated with the need for human delivery of the training in order to ensure trust. This was further connected to the idea that greater levels of information awareness regarding general matters of ICT cyber security were best delivered using face to face means rather than by ICT information pages where the emphasis was on the information without a specific person or team. The most dominant theme in terms of seeking information was the need to have the choice to receive information in different ways, with the strongest preference being to receive information by means of face to face delivery.

6.8.3   Expectations for Problem Solving

In terms of Problem Solving themes the results point to four main areas. Table 6.46 showed the conceptualised main themes as connected to the idea about problem solving. Some of these are sufficiently connected to form the dominant themes that underpin these results. These main areas were the management of expectations in terms of online banking trust, multiple problems in terms of past experiences with security and trusted usage, training and capability improvement that is tailored to older

people, and the provision of online banking choices that are competitive with existing banking systems in terms of complexity, security, and customer satisfaction.

The themes relating to problem solving focussed on the expectation (or lack thereof) that ICT challenges in terms of trusted usage and acceptance could be solved. The themes explained above are also connected to an underlying theme of low expectations regarding the trusted usage of ICT online banking systems. The theme of trust in online banking is dominated by recollections by respondents about their experiences and/or the experiences of their older peers. Many of the responses cite failed experiences. The commentary regarding people who have been deceived or who have lost access to information is strongly connected with older people's perceptions that online banking and ICT usage in general is not as trustworthy as existing human-based experiences. Online banking is depicted as problematic.

Comments about what is required to trust online banking in a regular sense was strongly associated with many of the negative experiences mention above. These align strongly with issues of ICT complexity, likelihood of cyber deception, and the unlikely acquisition of sufficient ICT capability. There is a connection between trusted usage and acceptance of online banking and the low expectation that sufficient problems are solved to the satisfaction of older people. These issues are mentioned in combination with each other by participants.

The idea that emerges is that in order to accept, trust and use online banking, participants must receive adequate information and training through a method of their own choosing (ie. That includes face to face delivery), and with sufficient capability and training to recognise security issues with reasonable ease. The theme that dominates this section is that the problems of transitioning to online financial systems are overly complex and problematic, and that shop front banking retains greater levels of choice, security and satisfaction.

6.8.4 Summary of Interview Results

The results presented here revealed four main concepts. These concepts were derived from a process of coding that applied labels, linkages, and associations to interpret the meaning of different ideas against other ideas.

- The Concept of Trust in ICTs – related to adaptation.
- The Concept of Human versus Digital trust– related to adaptation.
- The Concept of Choice in Using ICTs– related to problem solving.
- The Concept of Trusting in Information via Digital means– related to seeking information.

The process was highly cyclical with the analysis of themes requiring the transition from the data back to the idea and back to the other data through multiple iterations.

Table 6.47 Summary of thematic results of respondent interviews.

Insufficient General ICT Capabilities and the need for improvement
Mistrust in Digital Information storage
Perceived vulnerability to cybercrime
Choices including face to face and human exchanges
Independence to interact with ICTs without the need for assistance or intervention
Trusted reliance upon Peer-derived information
Trusted information using specific brands
Management of Expectations about ICT usage
Competitive choices for ICT banking usage involving complexity, security and satisfaction
Training that is congruent with the beliefs and norms of older people
The impact of perceptions of past experiences with ICT security and financial losses
Expectations required for online banking trust

The dominant themes here are arranged in Table 6.47 and represent the multiple thematic inter-connections between the four main concepts derived from data collected in respondent interviews. The next chapter considers the data and results of the hypothetical scenario testing that was applied to the sample respondents and discusses a compariosn to the data and results of this chapter.

7 CHAPTER 7 DATA AND RESULTS FROM SCENARIO TESTING

7.1 Scenario Testing

This chapter discusses the data collected during the interviews of twenty-eight older people to ask them a range of questions in the form of hypothetical situations and "what if" circumstances. These interview questions used twelve scenario based vectors of inquiry. Chapter Six previously described the first four interview parts to the areas of inquiry with participants. In this chapter, the fifth section of interviews (scenarios) forms the area of inquiry, as referred to in chapter 6 (see Table 6.1). All of the scenarios required participants to consider aspects of trust, distrust, acceptance and rejection. The scenarios posed choices, impositions, and mandated events that related to opportunities to engage with ICTs. In each of the twelve scenarios, the choices involved a differing consideration of trust that focussed on mandates, impositions, obligations, and choices (Table 7.1).

Table 7.1 List of scenarios discussed with participants.

	Scenarios
1.	Change from paper printed bank statements to users downloading and printing their own bank statements
2.	Unexpected phone call requesting payment
3.	Forced to use online system to manage pension funds.
4.	Card appointment replaced with SMS doctor's appointment reminder.
5.	Patient health information stored on a mobile tablet instead of on a hospital chart.
6.	Holiday booking reliant on client online access & printing of documents & tickets.
7.	Credit card taken away (out of sight) for payment
8.	Prepayment of hotel for accommodation
9.	Free online statement offer
10.	Self adminstered online tax returns
11.	Free overseas calls but with ID record of a credit card
12.	Online grocery purchases with free delivery

Each scenario posed opportunities to engage in an online system that controlled a transaction. In some cases, it was in the form of a financial transaction and in some case it was in the form of an informational exchange. The scenarios were based on one of three levels of online trust. Some scenarios involved measures of online obligation, where the user felt obliged to use a particular system. Other

scenarios measured trust where a system imposed itself upon the user. Some scenarios involved technology usage that was mandatory. As with the interview data described in Chapter 6, respondents gave their answers verbally, and their responses were recorded using a digital recording device, which was later used in playback as a means of obtaining a transcript for each interview.

This final part of the five-section interview process asked questions centred on specific trust-related scenarios. The responses were recorded in order to gain insight into the way older people perceive technology and trust, and the differences between trusting ICT systems where there is little or no alternative.

7.1.1   Why Scenario Testing?

The interview data from chapter six focused on the experiences and knowledge from interviewing older people about their interactions with information technology. In this chapter the focus is on drawing from participants their thoughts, perceptions and knowledge based on scenarios. In many cases participants' answers explain their challenges as they discuss how they would handle situations where imposed and mandated ICT interactions are put forward in scenario form. In some cases, subjects would draw on past experiences or analogous situations to assist in explaining an answer. Scenario testing therefore draws out from respondents a combination of experiential thinking along with the germane norms and values that come to mind as responses are made (Vannette, Krosnick, Presser, Fealing, and Ruggles, 2017). Scenario testing is useful in data collections where change, (in this case the evolving changes in technology and innovation) are factors influencing the research (O'Leary, 2010; Cohen, Manion and Morrison, 2008).

7.2   Scenario testing

The use of scenario testing is an important method of establishing thoughts and perceptions about matters where a full range of experiences may not have taken place. In interview questions respondents answer what they do, how they have done things before, and what they think the situation is based upon. They respond from their personal experiences and the experiences of others known to them. In the case

of information technology and computing, the literature confirms that older cohorts of people are likely to have limited experiences.

The use of scenario testing allows participants to indicate their thinking beyond partial experiences with technology and into perceptions and considerations that are created in concert with the experiences of peers, and the contextual practises and involvements of the people with whom they interact (Kaner, 2003). The scenarios that follow draw on a range of situations and circumstances that are designed to inform this study about the key issues of trusted usage, trust reduction, and trust rejection. This study seeks to understand how older citizens make informed decisions about using ICTs in connection with financial interactions. By testing these scenarios against older people it is possible to learn what distinctions are made when ICTs are mandated or imposed upon older people.

7.2.1 Bank Statements and the shift to mandatory online access

In this scenario subjects were given an example where the access to posted bank statements became constrained "over time". The scenario starts with bank statements sent in the mail, then to the banks urging people to access statements online, then to a fee structure on postal statements and finally to a scenario where bank statements could only be accessed online. Subjects' responses were recorded.

The shift to accessing online statements is initially one of voluntary choice, where online statements are recommended in terms of environmental benefits (paperless record keeping), and in terms of giving information control to the online banking customer. "Over time" the shift to online statements becomes imposed, where banks actively suggest online usage by incentivising and encouraging customers who change to an online banking system. The third phase of trusted usage is theorised as a point where online banking is a mandatory practice, and the acquisition of statements printed on paper is ended, and where replacement printed statements become cost-prohibitive. Customers are forced to seek bank statement information through the usage of an online banking system.

Responses referred to the physical need to have access to a computer, as well as the risk in interacting online within an environment where there is uncertainty and where there is possible theft and unauthorised access to private information. Some respondents referred to the tangible aspects of a

printed bank statement, and the ability to hold greater trust in a printed statement than in an attempt to find information in an online setting. Other respondents noted that printed bank statements are superior because they can be trusted and are official documents, whilst different respondents cited the need to resist (and break away from) banks that attempt to make online banking a mandatory practice.

Some respondents described the stress and anguish in navigating an online banking system. Others refer to the stupidity of being coerced into using a technology (a computer) that they do not understand. Many, (35%) discuss the absurdity of doing bank work (printing and locating on online statement), when they are the customer and not the bank employee (Table 7.2).

Table 7.2 Rejection of Online Bank Statements

Rejection and Acceptance of Online Bank Statements	
Rejection and Acceptance	85% of respondents cited some form of disquiet in relation to the removal of the postal option of statements. Responses ranged from switching accounts and changing banking to begrudging acknowledgement of the removal of a reliable postal information service. 15% of respondents stated the expectation that using online statements could be achieved and that although forced to adapt, the change was achievable.
Expectation that choice would return	45% of respondents stated that they hoped or expected that choice would return, and that it would be possible to choose whether to use online statements or to receive printed statements via postal mail.
Irrationality	35% of respondents questioned why their bank would expect them to perform all of the related banking tasks such as using computer statements, printing them, and then paying for ink, printers and storage, when they were in fact customers and not bank employees.

The majority of respondents stated that they would refuse to comply with a requirement to use online statements. Some respondents cited the accumulated cost and burden of home banking, whilst others cited the challenge of knowing that their computer was sufficiently secure. *"Is trust the right word here? I mean I would do it – I would use online banking if I had to – because the bank keeps sending me a message that says to go on line – to save paper – or whatever they say – but I don't know whether – I suppose I would be a bit sceptical – I'd probably still do it – look it all up – but I'd still wonder in the back of my mind – is it totally safe and secure"* (Respondent 13).

Some of the respondents stated that they were surprised at the shift in the burden of work from what was previously done by the bank, but was now expected of customers. Several respondents made comparisons stating that they felt as if they were unpaid workers of their banks. *"Would I trust myself? Maybe. Would I trust a system at home rather than going to a bank? No. If they cut off the statements*

in the mail – then I'll go to the ATM and get the printed statements there" (Respondent 23). Many respondents showed a preference to receive printed statements, rather than having to print them at home, whilst others saw printed statements through postal mail as documents that carried greater weight, and were more officially recognise than a xcustomer's home printed statement. *"I rely on the statements to make sure that my account is ok. I don't want to go to online banking, I don't have any faith in that. I know it's cheaper for the banks – but it means more work for me."* (Respondent 28).

7.2.2   Sudden and Unexpected Phone Call seeking payment

In this section respondents were asked to consider a scenario where they receive a phone call from someone claiming to be from their telephone company asking for a small payment to avoid a disconnection. The caller asks for a payment ($42.37) at the time of the call, suggesting the use of a credit card to pay the outstanding amount. This scenario aims to collect responses from older people in relation to issues of authority, trust, and financial transactions over telephone calls.

The respondents showed variations in the individual approaches to evaluating the possible trust or mistrust in the action of being asked to pay a small overdue bill by means of an over-the-phone credit card payment. Responses were wide-ranging and demonstrated vulnerabilities in the way older people choose to trust people in telephone service payment scams, and the inability to realise the possible security risks in play. Respondents stated firm, more emphatic views in cases where the topic of discussion was about phone payments using a credit card (Table 7.3).

Table 7.3 Small Scale Phone Scams and issues of trust.

Trust-based decisions and telephone scams	
Distrust of an unexpected call & a specific "call to action".	75% of respondents spoke about their firm understanding of the importance to not use a credit card over the phone
Trust in a recognised brand name.	15% of respondents stated the they would trust the call because it was asking for a relatively small amount, and they would normally trust a call such as this because it came from a trusted brand in the form of Telstra
Preference to pay using a credit card	10% of respondents stated that they would definitely use a credit card because in cases such as this where the amount is relatively small, they can make a payment by using their credit card.

The majority of respondents stated that theu would not give out their credit card details over the phone. *"I'm not going to give my credit card number out over the phone if that's what you mean. I'm very good at paying bills on time, so this isn't likely to happen. If it did – then I would probably go to a Telstra Shop and see someone to pay the amount owing."* (Respondent 7). Other respondents indicated they trusted over the phone conversations regarding something serious such as a telephone connection. *"If it's a person from Telstra then I would pay it probably. I have had a call from Telstra before, and they were kind enough to let me know so that I didn't get disconnected. I have been disconnected twice before, and the experience was dreadful ... I would have preferred to get a call and be able to keep the phone going – because it's important for me to be able to make calls and to get them."* (Respondent 8)

Table 7.4 Small Scale Phone Scams and choice patterns

Choices exercised in dealing with telephone scams	
Call Telstra independently of unexpected Telstra call.	43% of respondents understood the value of safeguarding against a telephone offer by contacting the host business (Telstra) directly rather than replying through the unexpected and unsolicited telephone contact.
Reject the phone call and disregard mentions of Telstra	50% of respondents stated that they would safeguard against the probable fake telephone contact by choosing alternate means of payment or account reconciliation.
Choose to pay the scam call.	7% of respondents indicated that they would settle the amount by following the telephone caller's suggestions.

In cases where there was a choice (ie to give credit card details over the phone or to check about the overdue bill through other means), respondents made different decisions. The responses suggest that most older people are capable of exercising caution and risk avoidance in terms of financial security in instances where they have a range of choices (Table 7.4). *"This doesn't sound like something trustworthy. I would not assist Telstra with this. I'd probably refer back to my local branch"* (Respondent1).

Of the respondents 43% stated that they would choose to contact Telstra independently of the (probable) scam call. A further 50% of respondents stated that they would choose a different means of rejecting the (probable) scam call. Only 7% of respondents were predisposed to accept an ad hoc call for payment at face value and attempt to resolve the call by means of "over the phone" payment. The responses indicate that in instances where choices can be exercised, a range of different options may be beneficial in promoting "security-aware" considerations and actions.

7.2.3 Mandatory online access for Pension Funds.

In this section respondents are asked to consider a scenario where Aged Pension payments change to become a fully digital process and one that requires all users to go online rather than simply receiving the payment in their accounts. Participants were told that they could visit a Government office, but would still be required to make contact by means of going online. This scenario is designed to obtain responses for situations with older peers who will have limited online access, and where larger numbers of older people would be expected to adapt to an online system (Table 7.5).

Table 7.5 Reaction to Mandatory Technology Usage

Responses to mandatory changes regarding Pension Funds	
Opposition to a forced change of system	81% of respondents opposed the need to change from a system that was working for the purpose of disbursing pension funds.
Opposition to a forced use of technology (replacing an existing system with options for face to face or digital contact)	71% of respondents opposed the mandatory shift to obtaining pension funds solely by means of an online process.
Imposed Usage to achieve a paperless set of transactions	57% of respondents suggested that a paperless set of transactions were either burdensome or insecure.

Some participants responded that an existing (reliable) system had been swapped for a digital response option that was classed as either strongly imposed or seemingly mandatory in order to obtain access to a known and trusted funding system. Responses indicated strong opposition to the loss of choice, and strong disagreement with a change that forced older people to use a new technology to the exclusion of a pension system that previous did not require users to endure computer access and understanding (Table 7.5). Many respondents viewed the proposed change in terms of additional work for themselves, rather than an existing system where government employees hold most of the responsibility. *"Unhappy. It's another system where I would have to do extra work. It's a strange thing isn't it – when governments and banks want seniors to get involved and get online – but then they put in place things like this where it looks more like a threat than an opportunity."* (Respondent 5).

Respondents described the proposed additional activities as both burdensome and complicated. *"Devastated. It's bad enough that the current system of pension payments makes me feel like a beggar, but if I have to go online ... well it's just another way that the government will make me do their work*

for them... and who pays if I make a mistake? It's like I've graduated from retiree to part-time accountant. I hear ads that try and tell me that online banking and using computers will make my life easier – but the truth is that it's very complicated compared to what I am expecting. Why can't they just return to the way things were done before?" (Respondent 8).

Respondents stated that propositions such as this would be hard to trust because they are based on actions which are either compulsory or heavily obligated. *"Isn't that what they already do – and if not – I guess you'd have to go with it – I mean if that was going to be that the only way you could access it and know your statements – then what choice would I have? You keep asking about whether I trust these things – but I don't consider it trust because I wouldn't have any choice would I? So there's no point in thinking about whether or not I trust something. I have to use it."* (Respondent M13)

The findings from this scenario suggested that technology mandates c reduce the level of trust in the usage of that technology. The act of forcing users to obtain pension funds only through a digital (ie access to a computer) pathway raised questions of distrust in the use of such technology. For some older people, a technology that is forced (or heavily imposed) upon a user, is a technology that cannot freely be considered as a trusted technology (Table 7.5).

Some older people recognised authority in the form of an official document that is printed on paper. The document represents something both tangible, and official (by holding it and sighting it they can believe something to be true). The findings indicate that same recognition of authority is diminished when the printed copy is a reprint of an automated or automatically generated document. The results further indicate that he majority of respondents place far greater trust in a statement from the bank that is on paper and sent via postal mail, than they do in a statement that they print using online banking and that they print off at home (Table 7.5).

7.2.4   Trust in SMS Reminders

In this section subjects were asked to consider the scenario that at their doctor's (GP's) medical centre the receptionist no longer hands out a small card with the client's next appointment written on it. Instead participants are told that they would get a reminder SMS Text message sent to their phone.

Subjects were questioned for their reactions, and asked whether they would put their trust in the SMS reminder system, or whether they would write the appointment details down somewhere. Subjects were also asked to comment about whether they trusted SMS messages in general (Table 7.6).

Table 7.6 Acceptance, Trust and Usage of SMS Messages.

Acceptance, Trust and Usage of SMS messages	
Accepted SMS messages for Medical appointment reminders	15% of respondents accepted the usage of SMS messages for the purpose of medial appointment reminders.
Did not accept SMS messages for Medical appointment reminders	35% of respondents did not accept the usage of SMS messages as appropriate as their principle method of receiving medical appointment reminders.
Did not trust SMS messages for Medical appointment reminders	50% of respondents did not trust SMS messages for the purpose of medical appointment reminders.

The findings showed two main areas of differentiation. In the first instance older people make distinctions between accepted usage and trusted usage. Responses fell into one of three categories. In the first instance, 15% of respondents indicated that they accepted the usage of SMS's for medical reminders. *"I write the appointment down on paper – in my diary. I guess I trust messages – but I would always check in my diary"* (Respondent 3).

35% of respondents stated that whilst they sometimes receive reminders by means of SMS messages, they do not accept their distribution as their accepted method of communication. *"I do not take any notice of sms messages. If I have an appointment – I make a note of it in my diary"* (Respondent 2).

All of the remaining respondents (50%) indicated that they do not trust SMS messages for the purpose of appointments (Table 7.6). *"I trust myself to make a note of appointments. I am organised. Sometimes I will gladly take a card from the receptionist with the appointment time written on it. – Or otherwise I'll keep it written in my notebook. Either way this is an issue of what I do to record when my doctor's visit will take place. But to switch this to where I rely on someone else, and someone else's system, is a real problem to me. I mean, you seem to be suggesting that I not only abandon my own system for being on time, which I have relied on all my life, and that also I should somehow expect someone else to have the same level of care and attention to my medical care as myself. I don't think that's very likely, do you?"* (Respondent 8)

A second variation from the responses gives an indication of the differing practice of reliance upon SMS messages as opposed to the reliance upon older habits such as writing down appointments and using a hand held personal diary. Over 90% of all respondents refused to acknowledge that SMS messages were more accepted or were accepted more than other means of communication (Table 7.7). From this group of respondents, 27% were prepared to accept the usage of SMS messages, however whilst they could see the merit in the use of technology, all of this group still preferred to rely upon systems other than SMS messaging for the purpose of remembering medical appointments.

Additionally, a further 41% of respondents stated that they rejected technology such as SMS messaging. Instead these respondents relied upon written notes, diary entries, calendar entries, and by memory alone. A further 13.6% of respondents rejected SMS messages as being an inappropriate method of reminding older people about medical appointments. Small response numbers (4.6%), indicated that respondents found it difficult to know what to do in the event that SMS messages are transferred as part of email system (Table 7.7).

Table 7.7 Acceptance and Trust versus Rejection and Refusal.

Acceptance and Trust versus Reliance and Rejection.	
Older people who agree to accept SMS messages but who rely on other systems such as written notes or diaries.	27% of respondents indicated that whilst they are OK with the fundamental idea of an SMS message, yet they still rely on things such as written down notes.
Older people who do not accept SMS messages but use other reminders	41% of respondents indicated that they reject the use of SMS messages and instead solely rely on written entries, diaries, or their memory, for medical appointments
Trust messages that are in email form but not SMS text form	4.6% of respondents did not trust SMS messages if they come as a text message on a mobile phone, but agreed that they could believe in an email message of the medical reminder came in that form.
Reject SMSs outright	13.6% of respondents reject SMSs as an appropriate method of delivering a medical appointment reminder that could be relied upon.
Accept SMSs	9.2% of respondents agreed that SMS messages would be a suitable means by which to deliver reminders for medical appointments.
Hesitant towards SMS messages from unknown phone numbers	4.6% of respondents found it difficult to believe in an SMS reminder from a number that they did not recognise. This would prompt them to call their medical provider by telephone or in person to confirm the appointment

Some respondents stated that whilst they are agreeable with the idea of sms messages, they still rely on other appointment measures such as written notes. *"I write things on to my wall calendar at home. I will read a text message – but I wouldn't rely on it. I went to Royal Perth (Hospital) last year for my hip waited for 4 hours and then someone said that they'd sent me an SMS not to come*

in… I was furious, and it's not the way to treat people is it? – especially when you're not well" (Respondent 6).

A small number of respondents had concerns about the identity of senders of sms messages. *"No I don't need SMS messages. I don't trust SMS messages – because I'm not sure who sends them. Usually it's just an unrecognisable number."* (Respondent 18).

7.2.5 Tablets over Charts: trust in e-devices to record patient information

In this section, subjects were given a hypothetical hospital scenario where nurses in a hospital ward collected a typical range of patient information such as temperature, blood pressure, and heart rate and entered them onto a tablet rather than a traditional hospital chart. Subjects were asked how they felt in relation to moving away from written records into electronic records on a tablet. Subjects were each shown an iPad tablet with a spreadsheet on the screen (Table 7.8). This section was aimed at comparing the difference between home-based online users of ICTs and trained professionals as users of ICTs.

Table 7.8 Trust in professional ICT usage under mandatory conditions.

Trust in professional ICT usage under Mandatory Conditions	
Accepted technology usage by trained hospital professionals	65% of respondents accepted that technology used by trained professionals could be trusted and would be far more reliable than older people using the same technology.
Does not trust the use of technology over handwritten medical records	12% of respondents responded that they do not trust medical records that are recorded on a tablet
Concern that tablets that can be accessed and used by others (visitors, children, others)	23% of respondents held concerns that medical information recorded on a tablet could also be accessed by children, visitors and others, and therefore would be less reliable because records could be easily altered without a trace.

The findings showed perceived differences between scenarios where ICT usage was undertaken by professional staff (in this case nurses) who have received IT training compared with older people who are not using technology in a professional capacity. The responses showed that there was a difference between situations where a person uses ICT technology as part of their trained professional work environment and situations where older people use ICT technology in non-professional conditions (Table 7.8). *"Yes – I've seen it done. When I go in my doctor does it all – and then he can print it out too. I think its fine because the doctor is a highly trained medico and he will undoubtedly know how to use a computer … probably really well."* (Respondent 6). Many respondents stated that people in a

working capacity with trainng and skills were suitable users of ICT systems. *"I can't think of a problem. Let the nurses be as skilled as possible. Less paperwork and more use of IT sounds like a very good idea."* (Respondent 1).

Some respondents cited security concerns. The findings showed that the concerns were directed at where the tablet was left when not in use, and whether other, non-authorised persons would be able to gain access. Specific concerns were raised about children and the ability to lose information whilst children play with technology through mobile devices (Table 7.7). *"I'd be concerned about the safety of the information on the tablet, although I know that technology is going in that direction – and I know that it's probably more expedient – from the organisation's perspective. My concern is not about the digital record keeping that is becoming the norm, its more about the security of such information, where such a tablet is left or stored, in the reach of others – and whether it can be altered by others or accessed by others by means of another device or connection."* (Respondent 15)

Other respondents cited the issue of lost data, and mentioned the ease by which data could be erased from an electronic tablet (Table 7.8). *"If the information is entered into a machine and recorded then I guess its ok. But I'd hope that there is also a paper record ... something tangible in place. I mean if the iPad gets wiped – what then? Do we just let the patient die?"* I assume hospitals have a sensible approach to back up systems so that the patient information isn't just stored in a digital sense."* (Respondent 18)

Findings showed a general acceptance of the use of tablet technology for the recording of medical information. 64% of the respondents indicated acceptance of the idea that in a hospital their normal medical statistics (such as blood pressure, temperature, and O_2 levels) could be recorded using a mobile device. In some responses however, there were limitations placed on the trust that extended beyond the initial record taking (data entry), to an understanding about where the data would be stored and in what form. 23% of respondents stated that patient statistics using a tablet was reliable, yet the reliability of the data storage was limited, with additional need for paper-based records management (Table 7.9).

Table 7.9 Trust in Digital versus Paper medical records.

Trust in Digital versus Paper records	
Acceptance and trust in medical records being recorded as digital data	65% of respondents accepted that technology used to store medical records could reliably be stored as digital data.
Limited trust in medical records being recorded as digital data, provisional upon data being also recorded in print or as a written record.	23% of respondents responded that their trust in medical records stored as digital data held limitations, and that their strong preference was to see such medical records recorded using a tablet, but stored as both digital data and in a tangible paper-based form.
Rejection of the practice of medical records being recorded as digital data, direct preference for handwritten records.	12% of respondents did not accept the practice of medical records being stored as digital data.

The majority of respondents (88%) accepted the use of technology for stored medical records. *"If there are trained medical professionals who collect these measurements then they probably already know how to use a computer tablet – just don't ask me to enter my own blood pressure."* (Respondent 10). Some respondents made comparisons to cafes and restaurants. *"No problem, as long as they don't ask me to use the thing. I mean that's the way it's going now – everybody is using iPads… the café that I sometimes visit has a system like that – and the waiter puts the order in an iPad – he doesn't write it down."* (Respondent 11)

Most of these respondents felt that such a system could be trusted. Some others had small concerns and raised the possibility of using both records stored using ICTs and paper-based records. *"My main concern is that any measurements taken are recorded in such a way that they cannot be altered or accidentally wiped. So are you telling me that I can't simply change any of the information on an iPad? I think I can. Surely the act of writing down and recording patient information in ink is better than a system that can be erased and retyped any number of times? Give me a permanent patient record every time."* (Respondent 8)

7.2.6 Downloading expensive and exclusive digital objects for travel

In this section, subjects were asked to consider a scenario where they had an expensive ($8000.00 AUD) "Around the World" holiday that was booked and confirmed by a travel agent, but that required the respondent to download the tickets themselves from a special account. The access to the download was granted by means of an email from the travel agent that included a password and login details.

Table 7.10 Trust in online claims for airline flight tickets.

Trust in online claims for airline flight tickets.	
Acceptance and trust in download and acquisition of tickets	35% of respondents accepted that their tickets could be downloaded and acquired.
Rejection of the idea of downloading and acquiring online tickets.	65% of respondents rejected the idea of downloading their own ticket and expected the travel agent to complete this task

This section aimed to see what older people would think of a system where they completed the final steps of the transaction, and where the transaction was a travel product worth many thousands of dollars. The scenario deliberately chose a high value holiday so that they could more clearly see the difference between trust in certain people. Some people place low values onto digital objects, and this scenario aims to draw out people who have a different set of values that are dependent upon trusting digital systems and digital technology compared to face to face travel-related transactions. Many older people see the acquisition of financially high-value digital objects as being connected with paid professionals rather than something that should be entrusted to older people with little IT experience (Table 7.10). The majority of respondents stated that they expected a better level of service from a travel agent rather than an email that required them to download and print their own tickets. They expected the travel agent (in its professional capacity) to provide the tickets in a printed form. *"I'm not sure it's a good thing to email out passwords is it? I mean the bank doesn't even do that. My limited knowledge tells me that there is a security risk in doing this. Plus, if I'm spending that kind of money then I'd expect my tickets given to me rather that as some kind of self-serve."* (Respondent 4).

Many older people showed considerable concern about the idea of having to download one's own ticket. Only 8% of respondents accepted the idea of downloading and acquiring their own tickets. The remainder of participants rejected the idea of downloading e-tickets, and 32% of respondents were more convinced that the travel agent would normally acquire and print e-tickets. A further 28% of respondents felt strongly enough that they suggested the need to replace the travel agent. Another 32% of respondents cited security and IT incompetence as contributing to the lack of confidence and trust

that many older people experience in using ICT and in assuming the responsibilities of the transactions. (Table 7.11)

Table 7.11 Distrust where the user does his own downloads.

Distrust of own downloads.	
Acceptance of the need to download e-tickets	8% of respondents accepted that their tickets could be downloaded and acquired.
Rejection of the need to download e-tickets based on expected service and on the large expense	32% of respondents rejected the idea of downloading their own ticket and expected the travel agent to complete this task
Rejection in favour of New Travel Agent	28% of respondents stated that they would prefer to get a new travel agent.
Rejection of the need to download e-tickets as the customer rather than having it done by the travel agent.	32% of respondents rejected the idea of downloading their e-tickets based upon their lack of confidence and the risk of an expensive computer-related problem.

The majority of respondents felt that their travel agent would understand the expectation that tickets would be printed for customers, rather than expecting the customer to download and print tickets. *"Not a great scenario. I use a travel agent from time to time. I use them precisely to avoid having to do things like this for myself. If I'm going to download e-tickets and other things, then I probably don't need a travel agent."* (Respondent 9).

Many of the trust and rejection issues revolve around risk in terms of the security risks in dealing with an expensive financial object (in this case an $8000 set of tickets). At the same time, however, respondents rejected new technology where they were expected to actively complete tasks such as printing one's own tickets, and having to provide ICT resources. 27% of respondents rejected a system that imposed the need for older people to print their own e-ticket. 73% of respondents indicated decreased trust in a system that allowed access to expensive tickets by means of emailed passwords (Table 7.12).

Table 7.12 Rejection on basis of doing extra IT work versus Security Issues

Rejection of downloading online e-tickets.	
Rejection of imposed need to download and print	27% of respondents rejected the idea of having to print their own ticket
Rejection of an imposed system that sends out passwords by email	73% of respondents rejected any system that sent out passwords via email

Older people rejected the use of technologies where the key task involved the imposed usage of their own IT. *"Fairly annoyed I should think. I would expect that for that kind of money she could*

have everything ready for me to pick up from the travel agent. I don't like risky things at the best of times – but why would I ever want to do something so fraught with risk just before I go on an expensive trip? And I wonder who would pay if I deleted the tickets or lost the password? Its things like this that make me think the world has gone completely mad. We seem to want to rely on self-service computing than on the normal things we trusted other people to do." (Respondent 10).

Other respondents rejected the mandatory acceptance of a system that granted access to goods based on the acceptance of email communications that released password access codes. *"Why would a travel agent want to effectively put themselves out of a job?"* (Respondent 18).

7.2.7 Hotel clerk holds onto older person's credit card for long time during stay

In this section subjects were asked to consider a scenario where they stay at a hotel, and had their credit card taken away out of sight, and held onto. Respondents are asked to explain how they feel about trust in hotels, foreign travel, and hotel employees (Table 7.13). This scenario aimed to draw out responses to trust where associated with financial interactions in both tangible and intangible ways. The scenario was designed to identify where older people are reluctant with both the virtual challenges of technology that is forced or imposed, as well as the physical challenge of handing over a physical card. In this scenario older people are asked to face the prospect of an imposed transaction (ie: to pass over their credit card) whilst also thinking about the challenge of imposed and required online transactions.

Table 7.13 Limitations to trust and actions arising from imposed credit card exposure

Limitations to Trust: imposed credit card exposure	
Specifically seek out a manager	32% of respondents did not trust an arrangement whereby their credit card was retained out of sight, and their first actions was to directly seek out hotel management.
Follow the card behind front of house activities (ie refuse to allow card out of sight)	37% of respondents rejected the idea of allowing their credit card to be taken away and held out of sight. Respondents were prepared to follow the card (to behind the counter) if required.
Check bank statements	16% of respondents stated that they would repeatedly check their bank statements in anticipation of expected bank fraud.
Limit exposure using specific restrictions on card limits	15% of respondents stated that they would either limit the amount held on the card (some said to $500) or they would switch to a debit (rather than a credit) card.

The findings showed that different money strategies had evolved "over time". Many respondents (32%) were direct in their actions, citing the need to speak with hotel management over regarding untrustworthy practices (Table 7.13). Other respondents cited their concern about credit cards

being taken away and out of sight. *"I would not like to see the card go out of sight, but I suppose if I had to stay there – then I might not have a choice. I like to prepay for accommodation so that there isn't any fuss about that sort of thing."* (Respondent 6).

37% of respondents were prepared to follow the hotel employee to keep the credit card within their field of view. Other respondents (16%) said that they felt helpless, and resorted to constantly checking their bank statements in anticipation of finding evidence of bank fraud. *"I might try and find another hotel if I had something like this, but I daresay it might not be possible ... last minute and all. The thing is to ask for receipts and to just check your statements. There will always be criminal types who will try and rip you off, but if I use my credit card on a holiday – then maybe I would have it set up to only make transactions of certain amounts. I'm pretty sure that can be arranged. I stayed in a hotel in Albany a couple of months ago, and they used my credit card and took it away out of sight. I was worried about having it card skimmed, so I just check my statements. So far - so good."* (Respondent 7).

The remainder of respondents (15%) mitigated their risks by either placing limits on the amounts held on their credit cards, paying with cash, or switching to using debit cards where they could assign a specific amount of money from a separate, less exposed account (Table 7.13).
"I don't like the idea of anybody taking my credit card out of sight – or making a scanned copy – regardless of the circumstances – I would not trust anything about such a situation – and I would not trust a hotel that made such a situation occur." (Respondent 15).

At the core of the responses from participants is the challenge of trusting a system or practice that is both imposed or forced upon the user, and also well known to be problematic in terms of card fraud, financial fraud, and non-trustworthy in comparison to other payment methods and customs. The responses show that in financial transactions for older people, choice is crucial to trust, and that where choice is limited, trust is also limited (Table 7.14).

Table 7.14 Trust with imposed and mandatory payment systems

Trust with imposed and mandatory payment systems.	
Acceptance and trust of a retained credit card by a hotel	10% of respondents accepted the idea that a hotel would retain their credit card
Mistrust of a retained credit card by a hotel	37% of respondents showed mistrust of a system that required their credit card to be retained out of sight
Forced hand over of a credit card … and no trust	53% of respondents felt that the action was forced upon them, and that in such circumstances trust was unable to be considered.

The responses from this scenario depict how circumstances that force or impose certain actions are linked negatively with concepts of trust. In this scenario, the emphasis is upon the physical retention of the card, even though the ongoing concerns would require monitoring and ongoing online action to show vigilance towards anticipated fraudulent banking activity (Tables 7.13 and 7.14).

An important observation about the responses in this scenario is the intention to find hotel management. All the responses spoke of discussion with a person rather than acceptance of the imposed credit card retention. The findings showed that older people look to resolving financial conflict by means of face to face contact with specific people. 69% of respondents indicated some form of human contact as a method of resolving an unacceptable and apparently untrustworthy scenario (Table 7.13).

7.2.8 Hotel advising payment system before arrival at hotel

In this section older people were asked to consider a scenario where they are going away to stay at a hotel and the hotel advises the need to pre-pay for the accommodation. The aim in this section is to get subjects to discuss their thinking and intentions where the hotel has imposed a setting upon them. In this setting the respondents have not arrived at the hotel, so the notion of an imposed payment procedure does not carry the same mandatory elements as in the previous scenario. *"I don't think I would do that. I don't mind going into a travel agent – and pre paying then and there. But I'm not going to go online with a hotel from another country, it's too risky. And no I wouldn't know enough to know whether they would use my card and charge me with other things. I mean who knows what they might do if they know that they can use my credit card for charging out other things."* (Respondent 7).

The most common response (48%) was to transfer the risk to a travel agent to take care of the payment in advance. In this scenario older people looked to connect with a human interface (ie a travel agent) rather than an attempt to pre-pay in an online format (Table 7.15).

Table 7.15 Trust in prepayment of distant accommodation

Trust in prepayment of distant accommodation	
Preferred trust placed in Travel Agent	48% of respondents preferred to pay a travel agent in advance than to make a prepayment to a hotel directly
Preferred rejection of hotel conditions in favour of a different system	29% of respondents preferred not to use a hotel that demanded a prepayment up front. Respondents preferred to find a different choice of accommodation.
Preferred to pay without using a credit card	14% of respondents preferred to pay using cash rather than handing over information about a credit card.
Felt that they had no real choice.	9% of respondents felt that they had little to no choice. They accepted the need to make a prepayment – even though they did not entirely trust the idea of making a prepayment. Respondents felt that the system imposed little choice on them.

29% of respondents found the prospect too risky and opted to reject using the hotel altogether, in favour of a different choice (ie different hotel). *"No I wouldn't do this. I'd go inside a travel agent and book through them. Then I'd have some comeback. It is easier to trust a local travel agent – in your own city – than a hotel in another country or another state."* (Respondent 17).

A further 14% of respondents felt that they could make a payment using cash and that this would be better than using a credit card. The remaining 9% of respondents believed that they had very little choice. The findings showed that they accepted that there was a need to make a prepayment; however they did not trust the system of payments, but instead believed that the system that was imposed upon them left them with little to no choice. *"No I don't trust the hotels from foreign countries. I will happily pay a local travel agent – and that way they will have the responsibility rather than me. This transfer of risk onto me personally seems unnecessary, why would I want to take this risk on?"* (Respondent 8).

7.2.9 Bank offer of Free Statements

In this scenario subjects were asked to consider a situation where their bank offers a new smart-phone app for banking that includes free statements that can be downloaded onto any internet device (computer tablet smartphone). Respondents were asked to assess whether this gave them a greater sense of trust in mobile banking than before, and whether they would be interested in such an application. This scenario aimed to determine factors that might encourage trust and acceptance of online banking

opportunities. It was designed to identify customers that would rely on digital systems rather than human, face to face, contact. It also explored responses about the rejection, distrust and suspicion of technology offers from financial institutions (Table 7.16).

Table 7.16 Perceptions about human contact, customer work and online trust

Perceptions about human contact, customer work, and online trust	
Reluctant to become a customer doing work for the bank	44% of respondents felt strongly opposed to the idea of doing much of the banking work for the bank. Free statements seen as a lure to convince customers to do the work of the bank for the bank.
Preference to remain in a system allowing for human, face to face contact	25% of respondents showed a strong preference to banking that allowed for face to face contact. These respondents saw the lure of free statements as an attempt to drag them from traditional "in shop" banking to online, faceless interactions.
Lack of trust in online banking	31% of respondents stated that they had no trust in online banking. They preferred traditional banking practices as easier, safer, and more appealing.
Support for online and mobile banking	21% of respondents supported the idea of online mobile banking. 11% did not specifically identify the scenario offer as something that would make them trust the bank. However they retained their support in general to trust online banking systems.

The findings showed that older people considered the shift to online digital banking access as something that involved a greater amount of effort on the part of the participant. Many comments indicated strong reliance on paper-based records keeping that was required irrespective of access to digital records. Bank statements that were sent via postal mail were perceived as more accurate, more official, and safer. Responses (44%) showed a dislike for additional document management, record keeping, printing, and additional equipment as an unfair shift away from bank services that previously provided the same services themselves and at no charge (Table 7.16). *"You have to ask yourself, what's in it for me? I mean that's what the bank does. If they can get you to look at statements without sending them to you in the post – then they're winning aren't they. You suddenly become an unpaid employee. YOU check the statement, YOU print the statement, on YOUR printer, with YOUR ink and in YOUR time. If I had to change – then I would. I'm not completely scared of online banking – if that's what you mean. But I would like to change if I have a choice to use something where I'm not forced to be the banker."* (Respondent 11).

In line with the thinking that banks have shifted work and responsibilities onto their customers, findings showed a secondary theme in the dilution of face to face contact with bank personnel in favour of online systems. Of the respondents 25% of comments described a preference for human interaction. Responses indicated far greater trust in personal contact and interactions than in attempts to trust in

online non-human exchanges (Table 7.16). *"I'm not interested in offers to make me do all the work. I would prefer to go to a bank and talk to a person."* (Respondent 2).

A third finding indicated that 31% of respondents stated that they had no trust in online banking. They felt that traditional banking practices, where transactions are conducted in banks, were safer, more secure, and vastly easier to take part in (Table 7.16). *"Firstly it certainly wouldn't make me trust them more than before. Secondly it doesn't interest me. I want a bank that looks after the security of my money – and makes it available for me when I want it. The way things are headed – it sounds like now I'm an employee of the bank, using my computer and my time. That should be of interest to no body."* (Respondent 8).

The findings also showed concern for a lack of participant skills, and a low level of capability to undertake online financial transactions. Older people believe that their own ICT capabilities are less developed than others, and that they are putting their finances and savings at risk by engaging in online banking, rather than by using the banks traditional face to face services (Table 7.17). *"No I don't feel that I trust myself for that sort of thing – the phone is too small – I'm scared of it and I don't know if I'm doing it right."* (Respondent 6). *"No this wouldn't make me trust the bank. I'm not learning about computing so that I can get a job at a bank. I am perfectly happy going to my local branch for all of my needs. I don't understand why people would want me to do these things."* (Respondent 12).

Table 7.17 Capabilities, suspicions, and online acceptances

Capabilities, suspicions, and online acceptances	
Lack of skills, knowledge and capability to undertake online banking	37% of respondents felt strongly opposed to the idea of doing much of the banking work for the bank. Free statements seen as a lure to convince customers to do the work of the bank for the bank.
Overall suspicion towards attempts by banks to engage with online banking	49% of respondents indicated that they were suspicious or wary of lures such as "Free Statements" that appeared to be an attempt to get customers to switch more readily to mobile and online banking applications
Trust in online banking	14% of respondents stated that they held some feelings of trust in online banking systems even though they had low levels of skill and capability in using computers and tablets.

In contrast to the themes of poor ICT capabilities by older people, and of the sense of being lured to online banking, there are a small number of respondents (14%) who trust online banking, despite recognising their own poor ICT capabilities. *"No this wouldn't make me trust the bank. I'm not learning about computing so that I can get a job at a bank. I am perfectly happy going to my local*

branch for all of my needs. I don't understand why people would want me to do these things." (Respondent 12).

These respondents hold a long-term view that ICT progress is inevitable, and reconcile the need to draw older people towards the use of online banking and mobile financial transactions (Table 7.17). *"Ok so I've had a couple of offers like this just recently. I'm not confident using a computer, but if I was to somehow become more used to using it then I might make a change. It's all going this way anyway, but I don't trust my ability in using a computer enough to jump straight in. Maybe after I learn more about my computer. I just don't want to get hacked and lose my money. Umm the offer is interesting – But I'm not ready."* (Respondent 7).

7.2.10 Trust and Confidence in self-administered online Tax Returns

In this section subjects were asked to consider their trust in tax returns under the imposed conditions of self-administered online returns. The aim of this question was to understand how older people feel about sending information of a financial, personal and private nature under imposed or mandated conditions. The aim is to show comparisons between the users of professional services, trusted systems, and financial transactions and transactions where individual participants would hold the responsibility for the trust and the responsibility of the exchange of information.

In this section participants were given a scenario whereby they were expected to prepare and send in their tax return on line. They were asked whether they felt confident to use such a system, and to complete their tax return without the need of help from an accountant. This theme aims to determine how older people might behave when they have to complete financial online documentation that of great importance and that can potentially impact upon their income and their lives. This scenario compelled older people to question what elements of financial online interaction can be trusted and what (if anything) needs to be rejected or changed (Table 7.18).

Table 7.18 Online financial tax returns: trusts, risks, and human interaction.

Online financial tax returns: trusts, risks, and human interaction	
Risks in attempting an online tax return without same support	95% of respondents felt that the act of completing an online tax return carried a high level of risk. Respondents noted that lodging tax returns are serious tasks and are treated with a high level of attention and with the support of others.
Trust in their own support networks and connections	35% of respondents indicated that they relied on the help of others to support them during the important task of completing and submitting a tax return. Respondents cited partners, friends, social club teams, and a range of existing networks that they relied upon and whose advice they trusted.
Trust in Tax Professionals	61% of respondents cited that they use a tax professional, and that they could not complete an online tax return by themselves. They stated that they trust the services of a professional person specifically so that their tax is completed competently. Respondents also cited a lack of trust in online systems, in online tax scams, and in their own capabilities.
Trust in people	75% of respondents stated that they needed or wanted some kind of human interaction and assistance. Many respondents cited that online systems reduced the opportunity to interact with other people. The online tax system assumed a level of ICT skill above that of many older people, and denied them the ability to talk about their difficulties.
Stress	24% of respondents stated that doing their tax return was a stressful experience. These respondents made the point that converting to an online return made the task more stressful
Need for choice when ICTs are mandated	33% of respondents made connections between being forced to complete the task online, and the need for choices and alternatives.

The findings showed that older people are reluctant to take such action, and are confused about who or what to trust. Many older people are reliant upon professional services for their financial affairs, and are risk averse towards non-human information exchanges. Respondents noted that tax returns are extremely serious tasks. Respondents were cautious about using their computer. They saw the proposed method of an online tax return as risky. Many older people cited trust issues with the government, with online transactions, and with relation to online tax scams. Most respondents saw the idea as unnecessary given that the previous system had worked for many years. 95% of respondents stated that doing their tax return online was a risky endeavour (Table 7.18). *"I'm not going to risk this kind of event. I always go to an accountant. It takes 10 – 15 minutes. Imagine how many hours it would take to do my tax return using an online system. And who would pay for me for all of the stress it would place on me. When I go to my accountant he talks to me. We have a chat about my tax. Is there an online person who will do that for me… and if so how much would that cost?"* (Respondent 10).

Some respondents spoke of a reliance on the support of others to complete important tasks such as a tax return. Respondents cited partners, friends, social club teams, and a range of existing networks that they relied upon and whose advice they trusted. Respondents also cited that they felt little trust towards an online system which was difficult to share with their support networks, but which had the

effect of segregating them from the assistance and support of trusted others. There were 35% of respondents who cited that access to support people was important in order to trust the task of submitting a tax return. 75% of respondents stated that they needed some form of human assistance, support or interaction as part of their ability to complete tax returns.   Respondents indicated that such support came in the form of human, face to face exchanges, and was more easily available through existing social and professional networks than through online intyeractions (Table 7.18).

Many respondents (61%) cited the need for using a tax professional. Participants expressed difficulties in completing several components of a tax return. They stated that they trust the services of a professional person specifically so that their tax is completed competently. Respondents also cited a lack of trust in online systems, in online tax scams, and in their own capabilities. Respondents indicated that given the high significance of getting their return submitted without mistakes, the idea of completing such a task themselves and online seems out of the question (Table 7.18). *"We don't like the ATO but we trust them. As for doing my return online, no thanks. I'll use a professional for that. I would not trust myself. We've been submitting tax returns for many years you know. It's not as if we don't know the importance of submitting it all properly"* (Respondent 5).

Many respondents stated that matters such as these required human interaction. *"I received three emails from what I assume were scammers who emailed me to suggest that I could click onto their email for assistance with an overdue tax return. Whether it was a scam or the real thing doesn't matter. I prefer to talk to a person. And in the case of my financial security I am not prepared to place my trust in an email from someone I don't know. In this instance the email didn't even give a name – just a department title. The form from the Post Office is the official form… so I trust that. If they think it's the same on line they are crazy. I just can't take risks such as this at my age. At least with the tax form from the post office I can chat with the others at the club. How would I do that using a computer? I suppose I can just carry it into my Probus club with me can I?"* (Respondent 17).

Findings showed that stress was a factor. 24% of respondents cited that being forced to do their tax returns online made a worrying task more stressful. The results indicated that older people who are overall less skilled, less confident, and less comfortable to use ICTs, would feel increased stress. (Table

7.18). *"No faith in this at all – I've always stressed about doing my tax, but to add the burden of completing it on a computer… it's far too risky and it's simply absurd. How can I trust a government that forces such things onto us oldies? Are they offering a free 6-month course in computing too? I have an old computer. It's not connected to the Internet or the World Wide Web… I really think this is going too far… I give up."* (Respondent 2).

33% of respondents noted difficulties when being forced to complete an online task, and were critical of the need for choices and alternatives, rather than acknowledgements of technology rejection (Table 7.18). *"I wouldn't trust myself – and I don't have a choice but to use some form of return for the ATO – so if there was no alternative then I would give in to the demand – but I don't think this is the same as trusting them… nor is it the same as an online program that I might want to use. I would go to a bookkeeper. The one I use knows me – and has been helping me for many years."* (Respondent 16).

7.2.11   Trusting 'freebies' the case of the free overseas phone calls

In this scenario the subjects were given a scenario where they could get something for free if they used an online program. This scenario presented an opportunity to make "free" overseas phone calls, but with the need to use a credit card to initiate the deal (Table 7.19). The scenario aimed to see how older people described trust in an environment where there are alternative options and where there are choices about what each respondent would do.

Table 7.19 Trust in IT offers with credit cards

Trust in IT offers with credit cards	
Rejection of compulsory credit card usage	63% of respondents cited that the offer gave the impression of something fraudulent. Older people could see the offer as just one of many telephone choices. Respondents showed that they trusted technology choices where the offer was straightforward, but in cases where a participant was required to use a credit card, the compulsory need for a card encouraged people to reject the offer (and the use of the technology).
Trust in non-essential technology	71% of respondents indicated that they were suspicious or wary of lures such as "Free Statements" that appeared to be an attempt to get customers to switch more readily to mobile and online banking applications

Many respondents stated that ICTs needed to be straightforward in order for users to trust them. Many cited that in this scenario, the need for a credit card when the calls are free is a sign that a person should hold back from trusting such a system. *"I might try this – but having to supply my credit card*

makes me suspicious. Why would they need my credit card – unless the object was to somehow get to use my credit card – and that somehow I would end up paying something?" (Respondent 1). Others held views built upon multiple experiences that indicated the need for caution. *"No it's not for me. It sounds like a scam. And even if it's real - there are many other offers like this that seem identical and are not real – they are phony attempts to get money from you."* (Respondent 2).

63% of respondents described that the offer to make free telephone calls seemed unlikely to be honest. Several reswpondents stated that they had seen other telephone and communications technology and were convinced that they there should be no need for users to need to register a credit card. Several respondents were content to reject the technology and to look for other alternatives (Table 7.19). *"There's no such thing as free calls – unless you're doing something illegal or dishonest. I reckon some of these online offers are really just attempts to get you to use a program so that they can access your information and then steal money from you."* (Respondent 8). *"I don't understand why I'd need a credit card – If it's free – it shouldn't need a card. It sounds dodgy – and I say no."* (Respondent 4).

The findings showed that many older people (73%) described that this offer had a luring effect on others. Respondents indicated that they were suspicious or wary of lures such as "Free Statements" that appeared to be an attempt to get customers to switch more readily to mobile and online banking applications (Table 7.19). The findings showed examples where older people found it difficult to trust an offer that contained a generous opportunity, but that also involved mandatory credit card registration. *"Actually we tried using a program called Viper or Viber or something like that. Only because we could make contact with our daughter and the grandkids whilst they are in Europe. But I prefer Skype – there's no need for a credit card – trust it more."* (Respondent 19).

7.2.12 Online Grocery shopping with free delivery if you order online

In this scenario subjects were asked to consider using an online ordering system for groceries which had the added incentive of free delivery, as long as orders were placed online. The aim of this scenario was to get respondents to explain their likely acceptance or rejection of an online opportunity

that was not mandatory or imposed, yet included the compulsory action of ordering online in order to

obtain a free delivery (Table 7.20).

Table 7.20 Trust in online grocery shopping

Trust in online grocery shopping	
Trust that the service is of benefit	44% of respondents stated that this was a service that appealed to them, and that they would definitely use. Unlike in other examples, where the online activity seemed skewed in the provider's direction, the scenario here depicts a scene where the customer receives a tangible benefit (in terms of the grocery delivery) and the technology benefit of shopping online without leaving the house.
Trust in non-essential technology but not the motives	33% of respondents indicated that they were suspicious or wary of lures such as "Free Delivery" that appeared to be an attempt to get customers to switch more readily to mobile and online grocery shopping applications
No trust	23% of respondents stated that they did not trust the online grocery shopping app, and did not like using a computer for such a thing. Some older people held doubts about the system of online ordering.

The majority of respondents were in favour of the online grocery proposition. Several liked the

idea that there was an actual delivery person and that the process was a combination of ICT technology

and human delivery. *"It would be a fun thing to try once – but I think I'd prefer to select my own goods*

when I go shopping. Perhaps if I'm sick – and I need it delivered, I might resort to this, It's not like it's

a faceless transaction, ... I mean I'll still meet the delivery person wont I?" (Respondent 2). The

findings showed that different older people have mixed feelings about trusting online technologies. For

some people there is the fear that appealing offers such as free delivery (if you order online) is used as

bait to convert people into users of technology. This scenarios relates to a much weaker emphasis on

mandatory ICT practices (Table 7.20). *"Yes I'd trust this. Its sounds like a good deal. Free delivery,*

wow that's great." (Respondent 1).

For some respondents the opportunity to purchase online vegetables and fruit from the comfort

of home brought about questions of trust. 44% of respondents stated that they trusted the online grocery

app and that they were being looked after as customers of the grocery store (Table 7.20). The findings

showed that respondents found it easier to trust a system that had a local, physical presence (ie wasn't

fully virtual), and that provided a good service to people in the neighbourhood. This scenario depicts a

scene where the customer receives a tangible benefit (in terms of the grocery delivery) and the less

tangible benefit of shopping online without leaving the house. *"This sounds like a great idea doesn't*

it? I've heard about Woolworths doing this. I actually might give something like this a go. Especially if they deliver it to me. It's not like they want to steal my money." (Respondent 11). Some respondents cited brand-related trust. *"I would trust Coles or Woolworths. If it's a universal thing and it takes off – then that's ok. I think that's the sort of thing that can have a standing order – or an app. So it doesn't sound complicated. I could trust something like that – especially if everyone starts doing it. I'd still buy my own fruit though."* (Respondent 4).

Some respondents were more reserved in citing trust, however 33% were comfortable to state that they trust the technology use, even though they might hold a reservation about an offer that uses free delivery to lure people away from other forms of shopping (Table 7.20). *"No – I like to shop in person. I might trust this program – but not the supermarket. How would they know the level of ripeness that I might want to buy? Why don't they just let you ring through an order for a delivery, just like the pizza places"* (Respondent 9).

The findings showed that for 24% of respondents the new ideas met with little acceptance (Table 7.20). For some respondents the opportunity to go to a store and physically choose and handle the produce that they wish to buy was described on the responses. *"I'll do my shopping the normal way. There are just some things that I can't see changing. Grocery shopping will always be an activity that will need me to go to the store."* (Respondent 8). *"I'm not interested in online purchases. There is always a risk that I could lose money. As a senior – I'm not looking to take greater risks. I would prefer to see what new innovations become permanent, and what are just fads. I don't think online grocery shopping can compete with my desire to pick my own fruit and my own vegetables."* (Respondent 18).

7.2.13 Summary of Scenarios Part 5

In the previous chapter (six) the first four parts of the interview data was discussed, showing the results of interviewing participants in terms of participant backgrounds, types of ICT usage by older people, descriptions of trust, and understanding concepts of trust (Table 6.1). In this chapter the fifth component of the participant data using scenario testing is outlined and discussed. In this section participants gave answers to a range of scenario questions that extended issues of trust using ICTs to progress into variations where imposed and mandated ICT usage was more clearly proposed.

Of the twelve scenarios tested three were directly related to matters of online banking, and a further five were indirectly related to banking but directly concerned with matters involving money and finance through the use of ICT systems. Of the remaining four scenarios, two scenarios were associated with ICT systems regarding health records, one was associated with free overseas phone communications, and the last scenario was associated with the ordering of grocery shopping by means of an online system. All of the scenarios proposed various online ICT usages that incorporated either imposed or mandated ICT usage. The results of the participant responses revealed a clearer view of how older people who are novices in the use of ICTs respond to online systems where choices are replaced with restrictions. The scenarios offered a range of circumstances that aimed to identify what areas are important to older people when making decisions about the trust and security of money and information, as well as the accepted usage of online systems in order to interact and engage within a modern progressive environment.

Table 7.21 Topics used for interviews for scenario testing

	Scenarios
1.	Change from posted bank statements to downloading & printing their own bank statements
2.	Unexpected phone call requesting payment
3.	Forced to use online system to manage pension funds.
4.	Card appointment replaced with SMS doctor's appointment reminder.
5.	Patient health information stored on a mobile tablet instead of on a hospital chart.
6.	Holiday booking reliant on client online access & printing of documents & tickets.
7.	Credit card taken away (out of sight) for payment
8.	Prepayment of hotel for accommodation
9.	Free online statement offer
10.	Self adminstered online tax returns
11.	Free overseas calls but with ID record of a credit card
12.	Online grocery purchases with free delivery

7.3 Conceptualised data and scenario findings

The scenario results brought about a clear understanding of the challenges that face older people in accepting ICT-driven systems for the management and control of banking, finance, and other important information. The themes from chapter six that were conceptualised to provide clarity of the challenges to older people revealed significant knowledge about the issues relating to imposed and mandated ICT usage.

The first scenario where banking statements become available only in an online form revealed that whilst people will adapt to the online access of banking information they remain apprehensive that statement information is no longer available by postal means. As an individual event, the removal of bank statements sent by postal mail is not a difficult circumstance to overcome. However the wider implications of posted statements are that individuals must now engage in online banking to gain access to their bank balances. In reality there are other options, users can visit their bank branch in person, or can print out balance receipts from an ATM machine. However the perception from several participants is that they are being forced to engage in online banking.

The second scenario where participants are asked to trust a phone caller claiming to be from Telstra requiring an over the phone credit card payment revealed that most people understood that giving out credit card details over the phone was risky. However, a small number of participants claimed that they would trust the Telstra brand and make an over the phone payment. Additionally, in the interviews with participants about responding to a caller claiming to be from a bank, a larger number of participants stated that they were unsure about whether the caller could be trusted, whilst other respondents were concerned that they were required to give their personal details over the phone, despite assurances that their bank would never ask them to discose their private information over the phone. In this scenario, some older people feel obliged to continue with phone calls from people claiming to represent an authority such as a Bank or a Phone. In these scenarios the imposed expectation to engage with an otherwise unknown telephone caller reveals that older people interpret phone calls as events that require immediate action rather than situations where the call can be stopped and a respondent can verify the authority of the call and the caller through a previously trusted bank branch or utility office.

The third scenario where participants are informed that they would need to interact in an online system to obtain pension funds met with widespread disagreement. Most respondents stated that there was no need to change from an existing system that is perceived by respondents to be effective and something that does not require change. In this scenario many respondents claimed support for the need to retain options for face to face contact if required. The results of this scenario showed that when significant amounts of money payments are involved there is a strong preference for choice and alternative action rather than a mandatory system that forced online engagement. In situations where

older people interact with a regular exchange of money, they become concerned that the transactions involve greater risk because contact options become limited. In the interview data, some respondents cited that email contact details that failed to give an individual contact name, but instead gave out a generic non-specific position description held less trust than contact details for actual people. Broad email contacts such as *complaints @dss.gov.au* gave respondents the perception that they had little or no choice but to contact a department by means of an email, when those respondents would have preferred to speak to a person and to know their full name. The imposed nature of such interactions gave respondents the perception of a lower the trust in using a non-specific email contact, whilst at the same time reinforcing the perceived need for face to face contact arrangements.

The fourth scenario asked respondents about their willingness to be reminded about a medical appointment by means of a sms text message. In this scenario, whilst there were many people who agreed to receive a sms text message, there were large numbers of respondents who did not see sms messaging as the more reliable method of making note of a medical appointment. For many older people, their preferred method of reminder was the use of their own system using diary or calendar reminders. Since in this scenario the acceptance of a sms text message was voluntary, there was widespread agreement to receive a sms. However the majority of respondents also stated that they preferred to use an existing trusted non-digital system that placed trust in their own practices and habits than to change to an ICT system where they relied on an ICT system rather than someone that they knew.

The fifth scenario asked about respondents feelings towards swithching from hand-written medical charts to digitally recorded tablet stored patient records. In this scenario the responses favoured the use of mobile devices over paper records. The notable difference in this scenario however, is that unlike other scenarios that placed imposed and obligated opportunities on respondents, this scenario described responses about the use of ICT systems by trained medical professionals. This situation revealed that older people are satisfied in the abilities of medical professionals who have received training and who have the technical capability to use mobile devices to enter and manage medical records. In the interview data respondents who spoke about their hesitation to engage in online banking stated that they did not want to be treated as if they were unpaid employees of the bank. In this medical

scenario respondents were in favour of others engaging in the important use of ICTs because they were acting in a trained and professional capacity. Respondents trusted the use of ICTs for the recording confidential medical data. However some respondents pointed out that whilst the trusted acceptance of ICTs in the hands of medical professionals was appropriate, the expectation that older retired ICT novices would receive a similar level of trusted ICT usage was not appropriate.

The sixth scenario posed the situation where customers would need to download, print, and secure their own travel tickets for an expensive round the world trip. The majority of the respondents to this scenario indicated that the transaction was unnecessarily insecure, that emailing login passwords and expecting purchasers of $8000 worth of travel arrangements to download and print their own travel documents was inappropriate. Although this scenario drew mixed support for and against older people using their own ICTs to get travel documents, there was wider agreement that the practice of emailing download details as well as passwords for logins was an insecure practice. In this instance, where the usage of ICTs is not mandated and is only partially imposed, many respondents spoke in favour of rejecting the idea of downloading and printing the travel documents, and instead switching to an alternate vendor. This scenario revealed that where imposed usage of ICTs is presented as a trustworthy system, but is accompanjied by less trusted procedures such as emailing passwords and logins, that older people would, where possible, reject the usage of such a system, and look for alternatives.

The seventh scenario discusses the interactions that can occur where respondents are asked to use a system that requires the trust of an unknown hotel clerk, who takes the user's credit card away and out of sight. Although this situation is not directly linked to trust in ICTs, this scenario reveals an example of where the trust in a financially important system is imposed on the basis of the respondent's need to secure overnight accommodation. The responses revealed that participants were aware of a variety of alternative ways to retain fincnial security, and that this type of situation had a range of optional strategies that changes the situation in relation to trust and security. Where the respondents were able to articulate various optional strategies, a greater expectation of the use of secure transactional behaviour became evident.

The eighth scenario describes a situation where the user is expected to prepay for overseas hotel accommodation using a credit card. In this scenario respondents defined a range of strategies. However

there was significant agreement that prepayment for accommodation was an acceptable circumstance, and that there were a variety of trusted and secure systems in place to allow respondents to feel safe in the prepayment of hotel accommodation using a credit card. In this scenario the voluntary nature of this scenario proposition meant that respondents readily discussed alternatives such as cash payments and debit card limits. This scenario revealed that in a non-mandated situation older people were able to suggest options that focused on the trusted security and usage of their money in rtelation top planning overseas accommodation.

The ninth scenario describes an imposed offer to use a new phone-banking application, with the added inducement that those who take up the offer will receive free statements sent by email so that they can download them. This scenario uses an offer to convince respondents to interact with a phone-banking app. In this kind of situation the emphasis is on encouraging older people to engage in using an ICT system (phone banking) in stead of banking through older conventional means using physical banking facilities and being in receipt of posted regular bank statements. The scenario is depicted as an optional offer. Removing imposed or mandatory conditions on an offer to use an ICT has the effect of reducing ICT rejection, and replacing it with a wide variety of responses. Over 40% of respondents stated that they did not want to become unpaid employees of the bank. Several cited the cost of equipment, the need to buy peripheral equipment such as a printer. Nearly a third suggested the need to retain a face to face arrangement with their bank. At the same time over a fifth of the respondents stated support for online banking applications. This scenario revealed that the retention of face to face banking as an important strategy that retains trust in people and systems.

The tenth scenario proposes that all tax returns must be submitted online to the Australian Taxation Office. Whilst online systems for tax returns have been in play for several years, individuals have always had the option to submit their returns in a paper-based format without the need to submit online. The results of the data galvanised the responses into two distinct groups. Some respondents held no major concern, stating that they were already submitting online by using a registered tax agent who submitted online on their behalf. Other respondents were adamant that they would not do an online tax return because it was too risky. Many of these respondents cited that a tax agent prepared their return, but that the respondent did not submit anything on line.This scenario revealed that many respondents

perceived preparing their own tax return using an online system was too risky. Over 60% of respondents cited the need to use a trained professional in the form of either a tax accountant or a tax agent. Only one respondent stated that they were prepared to attempt a tax return without some form of assistance. The scenario demonstrated that the trusted use of an online system in relation to a financial matter required trust in ones own abilities as well as trust in an ICT system. The large number of respondents who relied on tax accountants further underscores the importance of trust as something that can be slected or chosen, and not something that can be mandated. Online systems that dealt with individual person's money require them to trust their skills and capabilities, as well as their trust in online systems.

The eleventh scenario deals with an online opportunity to get free international phone calls using an ICT system. The offer is conditional upon users giving their credit card details even though the offer stated that calls are free. In this situation respondents did not support the hypothetical offer, citing distrust, likelihood of a financial scam, and unnecessary risk in comparison to known free services like skype. In this scenario no mandated or imposed conditions were included. Respondents were able to offer alternative options for international phone calls, and as a result a variety of suggestions were made as part of the interview responses.

The twelfth and final scenario discussed the opportunity for respondents to place their trust in an online grocery shopping system. The situation offered free delivery based on the condition that respondents placed their orders using the online shopping program. This scenario was perceived as an attractive proposition by many respondents. It gained support because it did not mandate usage. Respondents were free to choose to use the ICT system if they wanted. The scenario revealed that there was strong support from respondents, based on the opportunity to try an ICT system under minimal risk conditions.The system did not place large amounts of the respondents' money at risk, and some respondents noted the benefit in trying an ICT system that could be used in a one-off condition, compared withother grocery systems, and could be used or rejected at the users judgement.

7.3.1   Summary of scenario and conceptualised data results

The scenario testing revealed marked differences between voluntary situations and events where imposed and mandated conditions changed the nature of respondent trust in terms of ICT usages. In

situations where there was either voluntary or lightly imposed direction towards an ICT usage, respondents were able to exercise individual (and varied) judgement in relation to other criteria such as cyber risk, self capability, informed choice, brand reliance, and peer advice. In mandated situations from scenarios, issues of trust were judged more carefully against risks, financial losses, and events that would impact on the circumstances of individual respondents.

The next chapter discusses the findings revealed in this study, in relation to the trusted usage of ICTs by older people under mandatory and imposed conditions. It does with a specific focus on the trusted and secure usage of financial ICTs in the form of both IT systems as well as ICT devices.

8 CHAPTER 8 FINDINGS AND DISCUSSION

This research study investigated the trusted usage of ICTs by older Australians, and the connection between mandated and imposed ICT usage, in relation to financial matters such as online banking. Utilising qualitative methodologies, data was collected from interviews with twenty eight participants over the age of 60, who had low levels of experience with ICTs. In this chapter, the key findings are discussed against the background of previous research, in order to reveal this study's contribution to the body of knowledge about mandated and imposed usage of ICTs in terms of trust and security.

The research question for this study asked what influences the way older citizens make informed decisions about trust in those ICT innovations that involve imposed or mandated online financial interactions. This study has revealed three key findings that associate strongly with the hypothesis that underpins the impetus for this work. The research question required an investigation into how older people interacted with ICT both in terms of financial interactions as well as in non-financial interactions. The question also required an analysis of the ways in which older people differentiate between voluntary ICT usages as well as imposed and mandatory ICT usage. Additionally, the research question called for an understanding about the different ways older people trust ICT usage, especially in understanding their dependence upon ICT systems compared to their trust in people who assisted in ICT usages. This study also sought to understand how older people learn and acquire skills, capabilities, and knowledge about the usage of ICTs. Moreover, it considered accessibility to ICTs for older people.

The study examined the norms and values that older people associated with in terms of trusted ICT usage. Additionally, the research question included an understanding of the risk appetites of older people in regards to financial transactions and the trusted usage of ICTs. The study further examined whether ICT usage was viewed by older people as convenient and helpful or whether it was burdensome and difficult.

Finally, a summary of the main findings that emerged from this investigation is reviewed, highlighting the contribution that this study brings to knowledge concerning mandated and imposed ICTs and their impact on trusted secure online banking interactions. The summary also addresses the

use of imposed ICTs in situations where trusted usage is a contested descriptor for trust in humans versus trust in ICT systems.

8.1.1   Key Finding 1. Voluntary ICT usage versus Imposed and Mandatory ICT usage.

This key finding provides an insight into the relationship between trust in ICT usage and the type of choice associated with that usage. The finding highlights five key factors that impact on these interactions. Firstly, trusted usages of ICTs were classified as either something that could be chosen or something where the perception of choice had been removed. Secondly, older people held differing and divergent views about ICTs in cases where the ICT usage could be chosen, compared with ICT usage where there was either no choice, or the implied sense that the choice was of little consequence. Thirdly, choices to use ICT systems and devices instead of performing face to face interactions were classified either in terms of trusted usage, or as usage that held diminished trusted credibility since it was underpinned by imposed or mandated conditions. Fourthly, older people evaluated their forced usage in terms of their own skills, capabilities, and knowledge to determine whether interactions could be attempted successfully without the assistance of others. Fifthly, older people judged imposed and mandated ICT usage against their pre-existing norms and values, in some cases making comparisons between successfully functioning non-ICT systems and mandated ICT systems. These judgements lead to acceptance of ICT usage in some cases, but also on occasions lead to the rejection of ICT usage. The impact of mandated and imposed ICT systems goes beyond simply limiting trusted ICT usages, it also leads to ICT-based interactions where the user follows an imposed pathway without fully understanding the security implications that accompany online financial activity.

The following explores key factors that were associated with trusted and secure usage of ICTs in cases where the usage was either imposed or mandatory. These findings are discussed in association with previous research and reveal fresh knowledge identified by this study.

The impact of choice upon trust.

The motivation for older people to engage with ICT devices and systems is different from the drivers that stimulate the ICT interactions of other age groups. Older people have a more established

set of norms and values built over a longer time than those in younger age groups. This study sought the experiences and opinions of Australians over the age of 60. In general terms it meant that participants were focused less upon career development and more upon asset security and lifestyle choices.

Previous research (Mendoza et al, 2013; Brown et al, 2002; Benamati and Serva, 2007) informed this study about volition in terms of both theory and practice. The discussion on various theoretical models such as the Technology Acceptance Model (TAM), as well as other forerunners the Theory of Planned Behaviour (TPB) and the Theory of Reasoned Action (TRA), were informative, but found it difficult to account for ICT usage and acceptance in situations where the interactions were either mandatory or imposed. Benamati and Serva (2007) explained that usage and acceptance held greater value in cases where the trusted usage and acceptance occured under conditions of freewill and choice. An important finding in this study of older people with novice levels of ICT is that usage does not necessarily equate to trusted acceptance.

This study addressed the impact of choice and volition upon trusted usage. The interactions of older people in relation to trusted usage of ICTs identified the key factors that impacted on trusted usage. The discoveries are discussed with reference to previous research and highlight new knowledge recognised by this study. The findings revealed that older people make different assessments about trust and security depending upon whether their interactions with ICTs took place under mandated, imposed, or freewill conditions. Older people seek to make decisions about the use of ICTs as part of the way they manage important information. The decisions made in relation to the usage of online banking are crucial to older people of, or near to, retiring age. This study focussed on the impact of using online banking in order to determine the affect of ICTs upon older people who have been steered towards using technology systems instead of face to face banking practices. Such changes represent challenges for older people who have limited knowledge and understanding of ICT systems. Brown (et al, 2002) highlighted that older people using banking technology are often required to conduct themselves under compulsion, obligation, and other external pressures.

This study found that there was a significant difference between ICT usages that involved choices, and those restrictive conditions that made various parts of the online usage appear to be either

imposed or obligated upon the user. The results from the data revealed that once a component of an online banking system was forced to follow a specific direction, older people regarded its uage with caution and hesitation rather than with trust. One example is that older people found the proposition of using online banking without the benefit of monthly postal statements to be daunting. Older people rely on the regular postal statements as a trusted connection to their previous banking experiences. They use their postal bank statements as trusted sources of information that they hold to be official documents that are indisputably true. Statements drawn from an online system are, by comparison, less trustworthy because they are derived from the user's own work and not from a trained banking professional. They have been printed at home and are on standard paper without a company logo ro company letterhead.

Respondents showed concern and trepidation towards banking offers that offered 24 hour access and interaction using mobile banking applications. Banking companies are keen to reduce the cost of their face to face banking. They extend this idea by imposing the shift from postal mail bank statements to online requirements stipulating that a user download their own bank statements using their own equipment. Many respondents described their dislike at becoming an unpaid bank worker, having to pull down their own statements, print them off for themselves, and manage a range of secure ICT practices to avoid bank scams and attacks from malicious software.

The findings of this study also revealed that older people found ICT usage that had mandatory elements was harder to trust than ICTs where the usage itself was optional. Similarly, in instances where users felt coerced to use banking software on mobile devices, they found that the experiences incorporated higher levels of risk, greater need for knowledge and capabilities. This brought about a much greater transferred responsibility to the user than when previously regarded as a customer.

The findings of this study also revealed that older people would review their options in regards to their financial transactions. In many instances the comparisons between previous face to face banking experiences were held in higher regard. Any mistakes or data entry errors were those of the bank and not the customer. Older people deemed face to face banking to be safer and more secure.

One of the interpretations of face to face banking compared to online banking was in terms of burden and inconvenience. Older people had some level of savings that was usually their most important asset since it was what provided them with an income for living and expenses. Unlike younger cohorts,

older people are more in line with retirement than in an active working life. If, using online banking, they make a mistake, and then they have to bear the consequences of their actions. Older people are, in a financial sense, risk averse to the concept of doing their own banking transactions when they would feel safer, more secure, and far less burdened by visiting their local banking branch and having banking staff complete their transactions for them.

Findings from this study revealed that older people hold onto those norms and values that have been reliably trusted throughout their working lives. The switch in recent years to online banking systems does not easily align with those older norms and values. Banking offers that involve trading off face to face banking in exchange for 24 hour access are not considered helpful, but rather in some opinions they appear like cheap gimmicks designed to assist the bank to reduce costs such as posted bank statements.

The norms and values of older people are powerful factors in relation to trust and trusted ICT usage because they are reinforced by the thoughts and ideas of their peers. The findings of this study showed that many of the study participants relied upon the advice of their peers in terms of decisions regarding the trusted usage of ICTs.

8.1.2   Summary of Key Finding 1 and response to the research question

A summary of this key finding identifies the important factors in determining the impact of mandated and imposed conditions on the trusted usage of ICTs by older people. The findings showed that older people viewed their financial assets as critical elements for people no longer in the workforce and reliant upon savings and assets for their ongoing needs. The first factor is that conditions that restrict or remove choice have a negative effect upon trusted usage. It is important to distinguish between usage (that can be coerced and imposed as stand-alone online systems), and trusted usage, where the user has an understanding of the expectation of secure banking outcomes.

The respondents in this study viewed coerced usage of online banking as detrimental to a trusted outcome. Many respondents spoke of their decreased options to view bank statements and their imposed requirement to use online banking to view bank statements and balances as a reason to either reject an online banking system or to find an alternate system. Respondents who spoke of the transition from

face to face banking into online banking revealed their preference to be able to access banking information through a range of choices, rather than one single enforced pathway. The findings showed older people who had neither the skills nor the training to engage safely or securely with online banking, and who were reliant upon the assistance of others to achieve access to banking information. The shift away from face to face interactions and the mandated restrictions of information access make a clear case to show that imposed and mandated online banking interactions may increase the volume of online usage, but at the same time reduce the trusted usage of ICTs engaging with financial banking.

In some cases, such as the requirement to use an online mobile banking app, the requirement to pull down banking statements from an online account instead of receiving statements in the mail is interpreted as a cost saving measure by the bank. Older participants in several imposed and mandated situations see little or no benefit in using online banking.

The second factor is that mandated and imposed usage of mobile banking requires some older people to learn new ICT skills in order to participate. Those who are novice ICT users are at a disadvantage. Older people rely on their financial assets and the security of their banking because as older people they are less likely to return to the workforce. "As such" they are vulnerable in cases where a novice ICT user might accidentally make a transactional mistake.This study revealed that older Australians are concerned that there is an expectation that individuals will develop ICT skills and proficiencies to the same level as banking staff. Older Australians see the expected development of advanced online banking skills as challenging, and provide further reasoning for them to retain preferences for non-ICT related banking practices. This preference is so as to allocate critical banking tasks to highly-trained paid professionals rather than older Australians with reduced levels of training, novice ICT skills and low capability in engaging with online banking in a secure and trusted sense.

The third factor is ICT usage that is derived from coerced and imposed conditions. Under such factors it is difficult to trust forced usage to the same level as ICT usage which is unrestricted. When older Australians are asked to leave behind previous banking experiences in exchange for online ICT usage, they form comparisons between face to face banking experiences that have been trusted for many years, and ICT systems that are newly operating, require greater effort on the part of the user, and are subject to greater variations of security breaches than previously described. Findings from this study

revealed that older people feel disadvantaged by the need to change from a previously understood and secure version of banking to an online activity which carries greater risk.

The fourth factor is that older but novice ICT users have widely different levels of experience, and unlike others, receive very low levels of structured learning. Skills and capabilities may develop at a slower pace to other age groups, and as people age they can become slower to adapt to new technology. The rapid pace of online innovation and development is evolving at a faster pace than some older Australians, and the expectation that older Australians will adapt to new and innovative ICT challenges in line with the pace of new innovations was revealed from the interview data of participants.

8.1.3   Key Finding 2 – The nature of Financial and Non-Financial interactions

This key finding provides an insight into the considerations of older people who are novice ICT users, by evaluating the differences in how older people treat financial online activity and non-financial online activity. The findings for this study showed that financial ICTs are treated differently to non-financial ICTs by older people.   The research question for this study asked how older people made informed decisions when using online systems.   The findings revealed that online usage of a non-financial nature was treated in a different way to financial online treatment. In the first instance most non-financial interactions in this study referred to email correspondence, social media usage, and document storage. Findings from the interviews show limited understanding of ICTs by novice older participants. Respondents were chosen as participants with limited experience with online systems. Whilst many had a fundamental understanding of how to send emails, differences between simple correspondence actions and higher level financial activies such as money transfers showed that simple online usage was achieved with a sense of trust because the activities were easier to understand and to action.

By comparison the much higher level activity of engaging in online banking had the effect of reducing trust because the users did not have an understanding of some of the important requirements to engage in secure financial online activities. The findings revealed a lack of understanding about security protection for online banking, the importance of a secure password, the ongoing requirement

to undergo training, and a sophisticated understanding of systems-based ICT usage without the benefit of face to face expertise and advice. The findings revealed that older people remained connected to the norms and values of a previous era of face to face banking, where trained banking staff performed money transfers and high level transactions, and where users placed their trust in the people working at the bank, rather than placing their trust in a system which they did not fully understand.

The research question focused on the need to understand imposed and mandated financial interactions and to make informed decisions about the trust in ICT systems. The findings revealed that older novices with low level ICT skills are unable to make informed decisions because they lack the knowledge, capability and skill to excersice financial banking to a sufficient level of complexity that they could describe their financial inetractions as trusted usage. The key finding revealed here shows that older people do not possess, nor do they desire to possess, a sufficiently developed understanding of the complexities of ICT-based online banking. The findings revealed that some users see banking professionals as the appropriate people with sufficient training to make trusted financial transactions. Many respondents cited their desire to make use of trained banking professionals for trusted transactions in preference to mandated and imposed usage of an online banking application. The findings support the need to offer a range of options when seeking trusted usage of financial applications. In situations where users are asked to trust their online interactions without the appropriate understanding of their actions, they may be unable to recognise that they operate within an environment that is vulnerable to the risk of online cyber-crime.

The findings highlight that for older people with limited understanding of ICTs, their interactions with ICTs that involved the movement or security of money resulted in different behaviour from non financial ICTs such as social media and email. Respondents described difficulties with remembering multiple passwords. There were many participants who stated that with too many passwords, they would routinely write down passwords as handwritten notes left beside a computer.

This finding revealed that older people showed more caution and restraint with financial interactions than with other ICT interactions. Interactions with social media, with email, and with mobile applications, indicated characteristically greater acceptance of ICT usage than with financially-associated ICT usage (such as online banking). Results from the participant interviews showed

widespread agreement with the ability to send and receive emails. Participants were interviewed about transferring money using online banking. The majority of respondents stated that they would prefer to go to a bank and get the transaction completed by a trained banking professional.

The findings of this study revealed that participants were not overly concerned with the storage of email and social media passwords in handwritten notes left around their house, yet when asked about an online banking activity, respondents cited caution and the need for up to date anti-virus protection, specific password protection for their online banking, and stated the need to prevent others from accessing their computer or mobile device.

Similarly, the study found that older people were less concerned about the safety and security of non-financial transactions than those where there was a possible loss of money. Older people were prepared to overlook various risks when they they handled non-financial ICTs. They were prepared to take risks with passwords, risks with information over the phone, and risks with information posted on social media platforms. In terms of online banking, however, there was a perceivable change in terms of risk. In some cases there was trust and acceptance, which was mostly in cases where participants were regular users. In the majority of cases, however, respondents would attempt to conduct banking using a bank teller rather than using an online banking account.

The literature describes resistance and hesitation to the use of banking applications based upon difficulties with the installation and comprehension of required protection systems including antivirus programs (Mattila, et al, 2003; Bhat, 2012; Festervand, Meinert, and Vitell, 1994; Faletti, 1985; Cymek, Burglen, and Minge, 2014).

Findings from this study revealed that participants often engaged assistance from a trusted friend or family member. In many cases though, there was the desire to reject ICT usage under forced or coerced conditions. The preference of many respondents was to make financial transactions through the assistance of bank employees. Many cited that an expectation of knowledge and skills capability with financial ICTs was unreasonable for novice users to attain. The expectation that novice users within an older cohort of people would acquire the necessary knowledge and capability was stated by many as unlikely, requiring significant training, and additionally a desire to learn.

The study also revealed that older people attached a sense of complexity (whether perceived or real), to using ICTs when making finaincial transactions. Previous research about financial ICT complexity (Mattila et al, 2003; Bhat, 2012; Festervand, Meinert, and Vitell, 1994; Faletti, 1985; Cymek, Burglen, and Minge, 2014) highlighted firstly, that older people were undecided and cautious about using online banking applications based upon the level of complexity involved in understanding the installation and operation of the application; secondly were guarded in their understanding and grasp of the required protections systems such as anti-virus programs; and thirdly were concerned that they needed training that was substantial in terms of learning, and that required renewal and update. The work of Moschis (1992) suggested that older people undergo psychosocial changes with age that partially explain their assessment of themselves as less capable to deal with complexities such as the demands of ICTs.

The literature describes resistance and hesitation to the use of banking applications based upon difficulties with the installation and comprehension of required protection systems including antivirus programs (Mattila, et al, 2003; Bhat, 2012; Festervand, Meinert, and Vitell, 1994; Faletti, 1985; Cymek, Burglen, and Minge, 2014).

The complexity of using ICTs extended into using other computers and devices, using machinery that was not their own, and that they were not necessarily familiar with. Complexity in this sense extended beyond using their own software of their own hardware, to having the extended capability to use other people's systems. Elder (et. al, 1987) coined the term technostress to describe older mature workers in government organisations with difficulty in using new and evolving ICT systems.

The sixth key finding demonstrates wide spread financial risk aversion. It reveals that within the range of older people who are novice at using ICTs there are many who have a decreased risk appetite to engage with online ICTs based upon their expectation, concern and worry that their online interactions represent an unnecessary risk when banking institutions and their employees are better trained, far more experienced, and are professionally engaged to perform banking transactions on behalf of others. The findings revealed repeated comparisons between the skill levels of older novice participants and highly trained banking staff. The findings further reveal that in some instances participants are willing to engage in online banking, but that the use of mandated and imposed

restrictions on instruments such as bank statements highlight the discovery of risk-averse older people. This finding of risk aversion for older people also contributes to establishing that mandated and imposed ICT systems reduce the desire to interact with the trusted usage of financial ICTs.

The seventh key finding reveals that older people see the task of trusting and using online banking applications as onerous, taxing, and worrying. The findings of this study revealed that older people saw the additional work as burdensome and inconvenient. Older people in some instances preferred to place their trust in trained professional banking staff. Mandated and imposed systems that prevent the inclusion of trusted professional staff force older people to become involved in ICT usage beyond the level that they may be comfortable with. They may prefer to use banking staff to perform transactions on their behalf, where the financial and technological risks and dangers are transferred from home users back to banking professionals who are paid to know and understand how to make financial transactions in a safe secure and trustworthy manner. The burdens of using technology may also include the cost of technology, the increased time and effort required to learn about technology, and the opportunity cost of ICT interactions that might be used in other ways.

8.1.4   Summary of Key Finding 2 and response to the research question

A summary of this key finding identifies the important factors in determining differences between financial and non-financial ICT trusted usage by older people. The findings show that financial interactions operate at a high level for older people, who rely on trust and security to ensure the safety of their financial assets. Older people who are retired have (in most cases) stopped earning the income stream from their working life, and instead rely upon their savings, superannuation, and assets to provide sufficient money to live.

Older people therefore look to make online financial interactions in situations where their financial assets are secure, and where transactions involving those assets can be made in a trusted and secure manner. The findings of this study showed a marked difference between financial ICT usage and non-financial ICT usage. The non-financial interactions revealed in the findings of this study predominantly indicate lower level ICT usage for the purpose of email communications, as well as social media interactions and document storage. In non-financial ICT usage, the user participants have a fundamental

understanding of how their non-financial interactions operate. Thus users can claim a level of understanding that supports trusted usage for non-financial interactions. At the higher level of financial interaction, the findings of this study reveal that there are seven financial usage factors that have an effect upon the way novice older citiens make informed decisions about trust.

The findings showed that older people viewed their financial assets as critical elements for people no longer in the workforce and reliant upon savings and assets for their ongoing needs. The first factor is that conditions that restrict or remove choice have a negative effect upon trusted usage. It is important to distinguish between usage (that can be coerced and imposed as stand-alone online systems), and trusted usage, where the user has an understanding of the expectation of secure banking outcomes.

This study presents findings that highlight the difference between trusted usages for financial ICTs compared with trusted usage for non-financial ICTs. The key findings in this section include differentiation between high-level financial ICT usages and lower level social media and email usage. The findings suggest that older novices do not regard themselves as being capable to match the knowledge, capability and skill of trained professionals, and that a high level of knowledge and skill is necessary to achieve trusted usage of financial ICTs. These findings also reveal the need to offer choice between ICT interactions and face to face engagement with banking professionals. Other findings in support of trusted usage and informed decision-making focus on security processes, the challenge of multiple passwords, and the need for high level comprehension of anti-virus systems and password protection.

An additional finding highlighted the reliance of older novices on trusted friends and relatives when undertaking online banking. The finding is a reminder that older people associate strongly with placing trust in other people. This study showed novices placing their trust in friends and relatives as part of their learning processes, as well as relying on trained banking professionals in preference to placing trust in online banking systems.

These findings associate strongly with the challenge of complexity, and the recognition that for older novices, there is a significant difference between walk-in shop front banking processes and home-based online banking engagement. One of the findings of this study highlights the difference in financial ICT usage, and the need to incorporate trusted usage through the inclusion of choice and voluntary

interactions with ICTs. Users attempting complex trusted ICT usage become aware that as a user their required level of knowledge and skill is insufficient to claim a level of trusted ICT usage.

8.1.5 Key Finding 3. Trust in ICT systems and Trust in people who assist

This key finding demonstrated the preference among older people to trust humans more than ICTs. The finding also suggested that whilst there was a low level of trust in ICTs from a novice individual user's perspective, the addition of another person to assist, control, or deploy an ICT, greatly increased the perceived level of trust in using a given ICT-based system. Older people associate their trust in the usage of ICTs more highly than when that usage is accompanied by the peers, professionals, or people with whom they associate trust.

Whilst the issue of help from others has already been discussed in the previous key finding, this study highlights the relationship between trusted ICT usage and the influence of people. Findings from the study showed participants who were reliant upon others for support, direction, knowledge and expertise. These examples of people-based trust reinforce the finding that ICT banking usage that restricts additional people-based interactions also reduces the level of trust in that usage. The findings of the study do not suggest that banking for older people becomes a reversal of practices to resume the engagement of banking staff as financial trusted professionals. The study highlights the need for choice and variety. Whilst mandated systems restrict choices, they also reduce trusted usage of systems. Thus a finding of this study is to recommend choices and voluntary options in critical ICT-based systems so that those in need of human contact and face to face interactions can associate within the social and cultural norms of one method of financial interaction whilst learning and adjusting to a different method of trusted usage.

8.1.6 Summary of Key Finding 3 and response to the research question

A summary of this key finding highlights the need to acknowledge the cultural norms and values of older novice Australians as they learn to interact with ICTs. Older Australians have limited training in the use of ICTs, but retain many years of experience in financial transactions. The research question

asks what effects older people with relation to trusted ICT usage. This finding recommends that ICT financial usages can improve through the development of choices that incorporate different types of financial ICT interactions. Placing a combination of trusted usage pathways that incorporate usage of ICTs as well as face to face trusted associates is part of a solution to the challenge of mandated ICT usage.

8.2   Summary of Key Findings

In the literature, older people are often characterised as belonging to either late adopters or laggards (Mattila et al, 2003). The findings from this research came about from an exploration of the way in which imposed and mandated ICT usage restricted choice, which in turn prevented ICT usage from being appropriately evaluated in terms of trusted usage. The findings of this study indicate that ICT usage in mandated systems does not become trusted usage exclusively by means of prolonged usage. Voluntary decision-making is also required to ensure that ICT usage can be either trusted or rejected.

The study highlighted that ICT interactions operate alongside non-ICT interactions. Older novice ICT citizens require the existence of choice in using financial ICTs in order to foster interactions that allow for unfettered decision-making. The inclusion of choice and voluntary systems allows ICT users to develop knowledge and skills that incorporate their own norms and values, and are also inclusive of new innovations and pathways.

The findings of this study highlight an elevated criticality for financial ICT usage. Mandated ICT usage increases financial risk to novice users of ICTs. The nature of mandated ICTs restricts the key factors that drive older novices to seek to improve their knowledge, skills, and capabilities in the trusted usage of ICTs. The findings of this study highlight the challenge of increased complexity in trusting ICTs as well as increasing the burden on users to develop sufficient skill and capability to safely and securely use ICTs.

9   CHAPTER 9 CONCLUSION

This chapter draws together the research and its outcomes. It explains the salient outcomes from the research and offers insights into future directions and further research opportunities. It highlights the important role that older people play in the ongoing spread and development of ICT technologies, and the need for further research. The findings of this study demonstrate that the trusted usage of ICTs allows older people to make informed decisions in competitive situations. Furthermore, it shows that mandated and imposed interactions with ICTs by novice, but older Australians can have the effect of reducing the trusted usage of ICTs, which can lead to reduced choices, the rejection of some technologies, and increase the risk of cyber crime.

The results and knowledge presented in this study followed a system of rational discussion. An extensive literature review identified the gaps where additional study was required and the review was used to consider the research question and the hypothesis that formed the focus for this study. In this case, the use of an action research approach enabled a systematic process of learning and explaining from the literature, from data and results by means of interview and scenario testing, and then to clarify more developed thoughts by means of a conceptual model. This study followed a process of action cycles that formed the scientific pathways in relation to the question of trusted and secure usage of financial ICTs by older people.

In examining the research question for this study the aim was to understand the choices made by older people when asked to trust mandated or imposed ICT technology. In particular, this study has, at its core, the objective of explaining the effect that mandatory technology use can have upon older people. By highlighting the compulsory usage of technology, this study can assist in the mitigation of insecure online behaviour when ICT users are forced or obligated to use online systems such as financial banking and online information systems. The research question therefore sought to understand how older people make informed decisions about trust in ICT usage when the systems being utilized include mandated or imposed usages.

The initial chain of literature review identified the Technology Acceptance Model (TAM) as important (Venkatesh et al., 2003; Davis et al., 1989). The significance was described as the concept

that all people will eventually accept using digital technologies and that in the case of older people it is not if, but when, they will accede to the financial needs. This study sought to test the idea that older people are simply at different stages of development, and that trusted and secure ICT usage is a choice rather than an inevitable outcome. The TAM literature suggested that older people will eventually join a mandated system (Venkatesh et al., 2003). This study aimed to challenge the notion that mandated technology usage guarantees to bring about trusted acceptance. The findings of this study suggest that technology development can and does move towards acceptance, but also moves towards technology rejection. Within these movements back and forth, the important question is not the broad ise of technology acceptamce. A more useful description of interaction is to follow the *trusted* acceptance of ICT usage.

9.1.1 The Significance and Impact of this research

This study was designed to gain a deeper understanding of online trust relationships for older people at a time when globally the world is experiencing increased numbers of older people. The practical importance of this study is based upon the need for change in the way new ICTs, new innovations, and new systems are rolled out to people through automated experiences that are imposed and mandated. This research demonstrates the need to carefully introduce new ICT banking technology through opportunities that incorporate choice and decision-making by older people. Systems that impose and mandate their financial innovations do so at their own peril.

The study recognised the importance of choice over mandatory ICT practices. The application of a conceptual model can be developed beyond financial apps and online banking to also include the secure protection and trust of informational innovations such as online elections, census taking, and data base management. The cost of failure through challenges to trust in ICTs can have a significant impact on economies. The 2016 Australian Census failure hinged upon the trusted and secure usage of ICTs. It cost the Australian taxpayer over $440 Million dollars (Byner, 2016).

9.1.2   Recommendations

This study has identified the importance choice in the diffusion of new ICTs and the need to restrict imposed and mandated approaches to new ICT system deployments. The study therefore raises several important considerations for future interactions requiring trust and security in ICTs. The 2008 Australian report on Financial Elder abuse demonstrated that online banking practices with mandated and imposed systems contributed to distrust in ICTs, insecure outcomes for elders at risk of abuse, and created a culture of resistance and caution towards the trust and chosen acceptance of online innovations. This study makes three recommendations that are supported by the findings outlined in chapter seven.

9.1.2.1   Recommendation One:

The developers of financial banking systems should include the option of human interaction and assistance, as well as personal characteristics such as names and individual contacts. The results from the data in chapter seven cited responses showing majority support of 75% for human contact details with mandated ICT systems (Table 7.18). Participants in this study stated that there was a high level of financial risk, and the need for human contact was important to allow novice ICT users to engage with the online system. In 2016 the Australian Census failed to capture all of the nation's data and an incomplete capture took place (Byner, 2016). The census was for the first time operated in both a paper mode and in an online mode, however widespread confusion from an imposed emphasis on using the online version of the census, in combination with inadequate numbers of telephonists at a nationwide call centre caused many participants to reject both the paper based and the online version of the census form.

9.1.2.2   Recommendation Two:

Banks and financial institutions should offer clear reward and incentive to customers for choosing ICT online options rather than punishing older users who seek to hold onto tangible banking components such as postal bank statements. The results of interview data discussed in chapter 7 highlighted that participants prefer rewards rather than imposed and forced usage systems. Table 7.20

showed an offer of free delivery for an online grocery system. Responses to the scenario testing indicated trusted support for the use of the incentive.

9.1.2.3   Recommendation Three:

Governments should pay heed to research showing that imposed and mandated one-off systems such as digital elections, census data gathering, and other government interactions are highly likely to endure online failure where the deployments include imposed, obligated or mandated usage of ICT technologies. One-off mandated and imposed events operate at a high level of risk because participants are predisposed to be suspicious of the need to impose a digital system. In contrast, the Australian Government successfully deployed a non-ICT system to the Australian public as an informal survey that involved a voting slip and a return paid envelope as part of the same sex marriage debate (ABS, 2017). The survey achieved widespread success with over 79.5% of eligible voters taking part in a non-compulsory survey (Schipp, 2017). The event highlighted the reversed results where ICT acceptance was rejected in favour of a postal system.

9.1.3   A Conceptual Model of Technology Trust and Choice

Models that predict the behaviour of those accepting technology have so far failed to allow for three main features that isolate novice older citizens. The first is that models thus far do not adequately allow for the specific variables pertaining to older people who are late adopters in ICT understanding. The second is that technology acceptance models do not fully appreciate (and give weighting to) imposed and mandated ICT usage. The third is that technology acceptance models do not adequately allow for the possibility of ICT rejection (on an equal basis to acceptance). This research seeks to understand why some people trust online banking whilst others reject ICT systems in favour of face to face financial interactions.

The Trusted Technology Choice Model for Seniors (TTCMS) model was developed as a conceptual model from an understanding of the need to reconsider the challenges of mandated and imposed ICTs, and to recognise that systems-based interactions can evolve in the usage of ICTs, yet can also evolve in non-ICT systems. By overlaying the Trusted Technology Choice Model for Seniors

(TTCMS) against ICT outputs (such as online banking) factors that associate with low trust, trust rejection, and / or usage under coercion can be recognised and treated. The presence of these factors would indicate the need to consider what ICT systems could be altered to promote trusted technology usage. The model shows the key factors as outlined in the study as determinants that explain where corporations and government departments can improve the likelihood of trusted acceptance through the incorporation of choice and encouragement, and through the restriction of mandated ICT usage (Figure 9.1).

9.1.4   Making Sense of the TTCMS Model.

The Trusted Technology Choice Model for seniors is a predictive model that can be used to forecast likely outcomes in the trusted acceptance or rejection of new technologies for older people. It is a deliberate attempt to incorporate the known challenges that older people experience when using technologies. In some cases this can be situations where users are transferring from a non-digital system to a digital one, such as the change from face to face teller banking to online banking. In other situations this model can be used where a user changes from one technology to a newer technology, such as when a user shifts from using desktop storage to cloud-hosted productivity services such as Office 365.

As such the TTCMS is designed so that providers of new and transformative technologies can take action to avert possible negative consequences before they occur. Previous technology acceptance models most commonly suffered from he false supposition that acceptance was simply a matter of time. Many models assumed that once a person had used a new technology – then sooner or later they would become accustomed to it and would then accept it. However the distinguishing feature of the TTCMS is that it considers usage and trusted acceptance as two different states. In making such a distinction it also incorporates the expectation that some users will not trust some technologies, and will reject the usage of those technologies if given the freedom to choose between usage and non-usage.

By combining data on the level of volition and imposition with a set of variables including risk, user capability, user skill, system trust, people trust, burden of use, guidance, accessibility, and user norms and values, it is possible to predict the chances of a given technology usage becoming trusted, adopted, or rejected. Technology providers who tap into these variables can then make more accurate

decisions about what levels of technology imposition are safe to deploy in order to create the trusted acceptance and adoption of a new system or technology use.

The model allows prediction using simulations with multiple scenarios. In financial technology use (such as online banking applications) the trust in people (such as bank tellers) becomes less important whilst the trust in the system reliability becomes far more essential. Similarly any reduction in the guidance and instruction for the technology use becomes problematic, and contributes to an increased expectation of risk and uncertainty. In the case of older people who have retired from the work force and who depend on their life savings more closely than younger people who still work for their income, the shift away from face to face banking and into online banking develops the need for unfailing systems reliability, in concert with a range of personal user requirements such as good guidance, developed capability and skill, and the ability to incorporate individual norms values and beliefs (Figure 9.1).

Since many technologies are deployed under imposed and mandated conditions, such a model is useful in predicting the additional features (variables) that will ultimately determine the trusted acceptance and ongoing adoption of a new technology. Older peope place great value on their independence, as well as their life's contributions in terms of information and assets. When the August 9th, 2016 Australian Census took place across Australia, the expectation from the Australian Bureau of Statistics (ABS) was that more than 65% of participants would switch to an online completion of a census form. However had they considered the variables and predictive features of the TTCMS it is possible that the ABS could have forecast that large numbers of particiants would reject the online technology use in favour of the paper-based system that placed a reduced burden, and required a lower level of technology capability and skills than its online counterpart (Australian Government, 2016). Although the 2016 Census gave people the choice between online submission and paper-based submission, the deployment strategy form the Australian government imposed the values of online technology usage over and above the value of door to door data collection. Deployment of the online system, which had never been done in Australia for a census, drew widespread criticism in anticipation of increased risks, low levels of assistance and guidance, reduced accessibility, and very low systems trust.

The model is derived directly from the data collected and analysed in this study. The terminology "not to accept" is retained in the description of the model because it has been lifted from the transcripts of several participants who explained their difficulties in using mandated and imposed technologies in terms of "decisions not to accept" or "not to reject" based on their usage under conditions where choice was either reduced or withdrawn.

The use of vertical and 45 degree angled arrows is important. Mandated usage and voluntary usage have a more direct impact on trusted acceptance or non-trusted rejected technology usage. In contrast systems where there was encouraged usage or imposed usage had an indirect impact or trusted acceptance or rejection. The model depicts "Volition" and "Mandation" as the strongest forces that determine forecast outcomes.

The central box within the model shows four grades of usage from voluntary, encouraged, imposed to mandatory usage. The dashed arrows leading to the factors show that the imposed and mandated usage of ICT triggers the factors in the top right of the model, whilst the dashed arrows from the voluntary and encouraged usage trigger the factors in the bottom left of the model.

The other quadrants reaffirm the loops that cite decisions not to accept and decisions not to reject. These arrows feed back to the reverse decision output – so that if one or more of the factors are not triggered – then a reverse decision is possible (eg: the decision not to accept or the decision not to reject). The model deliberately depicts the opposing nature of trusted acceptance and rejection in order to juxtapose both outputs as genuine possibilities – rather than the traditional TAM models that always favour the expectation of (eventual) technology acceptance. The model is (in this thesis) in its nascent form and is deliberately anchored to the data that forms its categories. It is possible that in future research and with greater revision this model can be shaped into a popular, more simplified version.

Defined Purpose, Limitations, and a useful representation of reality.

The defined purpose of the model is to assist people in predicting whether there will be better outcomes by accepting and trusting a certain technology usage, or whether there will be better outcomes by foregpoing or delaying the usage of a specific technology. The model is a simplified representation of the reality of how older people perceive technology usage as either trusted or rejected. It has many limitations, not least of which that there are many other factors that can influence outcomes regarding

trusted acceptance and rejection. However, based upon the data analysed in this study of older people. The model reflects the key elements that contribute to decisions about whether to trust, use, or reject an ICT technology.

Figure 9.1 The Trusted Technology Choice Model for seniors (TTCMS)
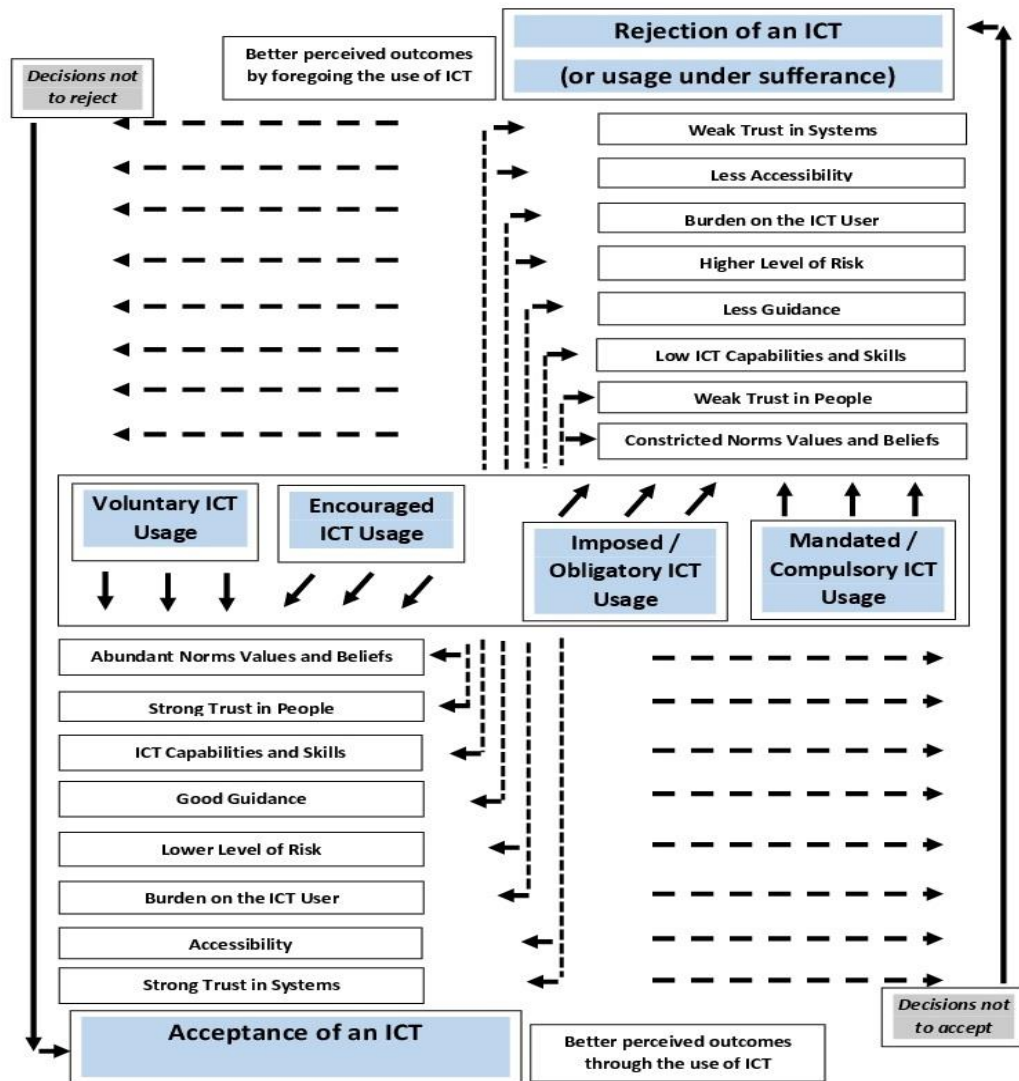
The model shows that Imposed and Mandated ICT usage can trigger a range of factors including weak trust in systems, reduced accessibility, burdening the user, increasing perceived risk, impeded by less guidance, reducing the desire to develop ICT capability, reducing the need to trust people, and restricting people's norms, values and beliefs. In contrast, the model depicts that Voluntary and encouraged ICT usage can trigger strong trust in systems, increased accessibility, less burden on the

ICT user, lowere levels or risk, abundant guidance, greater desire to develop capabilities, stronger trust in people, and the unhampered integration of people's norms, values and beliefs. Whilst the outputs seem binary, the model allows for varying degrees of trusted acceptance, partial technology rejection, and differing types of usage. In its simplified state this model predicts the trusted acceptance of ICT usage by older people when differing levels of forced usage are applied.

9.2   Conclusion

This study compared a range of ICT usages in terms of trust by older people as they interact with near-ubiquitous computing environments. The research aimed to predict usage and rejection decisions through the addition of mandatory, imposed and voluntary criteria. A novel conceptual model of technology choice for older people allows for mapping of informed decisions making that rely on trust and security under mandated and imposed conditions. Providers of critical technology in areas such as banking, health, and social services will be able to draw on the research to improve the level of trust in ICTs by older people. This study used a qualitative analysis of the behaviour of older novice ICT users in their interactions with mandated and imposed technologies, specifically where financial and high-order trust is involved. The research addressed the trust and security concerns of ICT stragglers who are generationally disadvantaged towards technology innovation. A specific focus of this study aimed to assist older people who felt compelled to accede to mandated and imposed ICT usage without sufficient regard to their safety and security. By understanding the key determinants that influence novice older ICT users, stragglers and late adopters can survive vulnerable and risk-based ICT impositions that limit financial and information-based choices.

The acceptance of new innovations should be based upon informed decision-making and freedom of choice (UNDP, 2013; Hammel, 2004). Mandated and imposed systems that assume ICT knowledge place the financial and informational databases of the world in the controlling hands of the few rather than the many (McLean, 2011). Good digital governance is predicated on social systems that breakdown power systems to provide broader transparency. Older populations make trust-based

decisions based upon their visibility of such governance (McLean, 2011; Rozanova, 2010). In many instances that means that an imposed system from a powerful corporation or government, challenges older people to evaluate the accompanying organisational structure alongside the innovation being rolled out (Katz, 2000; Minkler and Holstein, 2008). In 'mixed-trust' environments choices are complex, and mandated systems are less accepted than those that offer choice (Wicks and Berman, 2004; Jaeger and Fleischmann, 2007).

If society adopts a "one size fits all" approach to technology acceptance through the use of mandates and forced usage, then a growing population of older people is destined to become more disenfranchised from the use of ICTs. Mandatory ICT systems, along with heavily imposed systems, contribute to the rejection and distrust of technology and its innovations. This results in poor financial decision-making, insecure transactional behaviour and a range of obstructive and uncooperative interactions by older technology participants. The consequences of technology enforcement have wide-ranging impact upon older people. The effects range from assistive technology for older in the home, quality of life issues, and access to democratic rights in elections and voting. This study casts clarity and light on the contested issues of trust and security in technology, mandatory ICT effects, and the need to retain choices over enforced ICT usage in society.

Trust in technology fluctuates in relation to ICT usage that is mandated and imposed. For older people, compulsory ICT usage can have the effect of reducing trust in technology. This has the flow-on effect of reducing trusted ICT usage. Older people make choices to avoid and reject technology in instances where they perceive security risk and uncertainty within mandated ICT structures. The idea that usage of technology brings about trust and reduces financial risk is challenged in this study. Instead, the study posits a position that supports technology choices rather than acceptance mandates. The growing number of prominent failed ICT systems that force compulsory ICT usage support the proposition that trusted and secure technology usage is best predicated upon a foundation of choice and voluntary action.

Traditional forms of informational exchange retain an important part of financial decision-making. Older people (and all of society) interact with other humans to share and exchange ideas, information, and opinions. They make choices that are based upon trust in both people and technologies.

291

In the progression towards greater use of technology for its efficiencies and accuracies, it is important that information can be accessed through choice rather than through compulsory automation. The advantages of technology are only advantageous if they offer the same or better level of safety and security as traditional forms of information and communication. This study shows that imposed and mandated forms of technology should be carefully examined to ensure that existing structures, irrespective of their technology interactions, are not discarded or overruled by an appetite for technology usage. Trust in ICT usage has greater effect upon financial and informational outcomes than numerically superior accounts of usage.

Older people are described as laggards in technology usage because they are generationally limited in their knowledge of current technology. The rapid development of new innovations means that new ICT applications are embedded in younger generations but become outlying and marginal considerations to older cohorts such as older people. In this sense the term laggard is insufficient as a cohort descriptor in terms of ICT trust and security. The older person's cohort acts as an important brake and review of the inclusion of mandated technology systems. They demonstrate the use of choice and selection above enforced acceptance. Their review and discussion of new innovation and technology forms an effective appraisal and analysis of technology change. Their life position is unique, and qualifies them to offer important suggestions about financial risk and informational trust. They have the most to lose, with no options to recover from a life-time of financial and informational acquisitions. Whilst this study has specifically focussed on older people in order to understand the relationship between choice and technology, the themes and contributions to knowledge have application to any and all age cohorts. Older people's questions about trust and security hold value and significance to the improvement of trusted ICT usage and the retention of choice and selection.

10 Other Publications by the Researcher

Coldham, G., Cook, D.M., (2017), VR Useability from Elderly Cohorts: Preparatory Challenges in overcoming technology rejection. *Proceedings of the 35th National Information Technology Conference (NITC).* IEEE, Computer Sociert of Sri Lanka, Colombo.

Cook, D. M. (2015), Birds of a feather deceive together: The chicanery of multiplied metadata. *Journal of Information Warfare*, 85-96, Richmond, Victoria.

Cook, D. M., Kumar, A., Unmar-Satiah, C., (2015), Loyalty cards and the problem of CAPTCHA: 2nd Tier security and usability issues for senior citizens. *The Proceedings of 13th Australian Information Security Management Conference*, 101 - 111, Perth, WA.

Cook, D. M., Waugh, B., Abdipanah, M., Hashemi, O., Abdul Rahman, S., (2014), Twitter Deception and Influence: Issues of Identity, Slacktivism, and Puppetry. *Journal of Information Warfare*, 13(1), 58 - 71, Mindsystems 243 Bridge Road, Richmond VIC 3121 AU.

Cook, D. M., (2014), Identity Multipliers and the Mistaken Twittering of Birds of a Feather. *Proceedings of the 13th European Conference on Cyber Warfare and Security*, 42 - 48, Reading, UK.

Waugh, B., Abdipanah, M., Hashemi, O., Abdul Rahman, S., Cook, D. M., (2013), The influence and deception of Twitter: the authenticity of the narrative and slacktivism in the Australian electoral process. *The Proceedings of the 14th Australian Information Warfare Conference*, 28 - 38, Edith Cowan University, Joondalup.

Blanquart, G., Cook, D. M., (2013), Twitter Influence and Cumulative Perceptions of Extremist Support: A Case Study of Geert Wilders. *The Proceedings of the 4th Australian Counter Terrorism Conference*, 1 - 11, Perth, Western Australia.

Smith, T., Cook, D. M., (2012), Regulations for Retail Remittances: Compliance Entropy in Store-Front Transfers. *E-Proceedings of the 5th International Conference on Financial Criminology (ICFC) 2013*, 10-23, Universiti Teknologi Mara, Shah Alam Malaysia.

Cook, D. M., (2011), E-governance of the Forest: Management by Multivalence. *Common Property Resource Management: A Focus on Forestry*, 177 - 203, New Delhi, India.

Cook, D. M., Smith, T., (2011), The Battle for Money Transfers: The allure of PayPal and Western Union over Familial remittance networks. *The Journal of Information Warfare*, 10(1), 18 - 35, Edith Cowan University, Western Australia.

Letch, J., McGlinn, E., Bell, J., Downing, E., Cook, D. M., (2011), An Exploration of 1st and 2nd Generation CPTED for End of Year School Leavers at Rottnest Island. *Proceedings of the 4th Australian Security and Intelligence Conference*, 38 - 48, Perth, Western Australia.

Cook, D. M., Smith, T., (2011), Finance, Fear and Family: Issues of Trust and the Common Ground with Terrorist Funding. *Proceedings of The 2nd Australian Counter Terrorism Conference*, 1 - 11, Perth, Western Australia.

Cook, D. M., Szewczyk, P., Sansurooah, K., (2011), Securing the Elderly: A Developmental Approach to Hypermedia-Based Online Information Security for Senior Novice Computer Users. *Proceedings of the 2nd International Cyber Resilience Conference*, 20 - 28, Perth, Western Australia.

Cook, D. M., Szewczyk, P., Sansurooah, K., (2011), Seniors Language Paradigms: 21st Century Jargon and the Impact on Computer Security and Financial Transactions for Senior Citizens. *Proceedings of the 9th Australian Information Security Management Conference*, 63-68, Perth, Western Australia.

Cook, D. M., Smith, T., (2010) The Malarkey of Money Transfers: Overlooking E-Bay whilst the Hawaladars are Hunted. *Proceedings of the 1st Australian Counter Terrorism Conference*, SECAU Security Research Centre, Perth, Western Australia

Cook, D. M., (2010) Mitigating Cyber-Threats Through Public-Private Partnerships: Low Cost Governance with High-Impact Returns. *Proceedings of the 1st International Cyber Resilience Conference*, SECAU Security Research Centre, Perth, Western Australia

Cook, D. M., (2010) The Use of Governance to Identify Cyber Threats Through Social Media. *Proceedings of the 1st International Cyber Resilience Conference*, SECAU Security Research Centre, Perth, Western Australia

11 REFERENCES

Abbey, L. (2009) Elder abuse and neglect: When Home is not safe. *Clinics in Geriatric Medicine*, Volume 25, Issue 1 pp 47 – 60.

ABC News (2016) #Census Fail: Why people are worried about the census. Retrieved 4th October from: http://www.abc.net.au/news/2016-08-01/census-2016-why-are-people-worried-about-the-census/7678198

ABS. (2006). *Adult Literacy and Life Skills Survey*. Retrieved from http://www.ausstats.abs.gov.au/ausstats/subscriber.nsf/0/B22A471C221C7BADCA2573CA0 0207F10/$File/42280_2006%20(reissue).pdf

ABS. (2011). *Household Use of Information Technology, Australia, 2010-2011*. Canberra: Australian Bureau of Statistics Retrieved from http://www.abs.gov.au/ausstats/abs@.nsf/mf/8146.0.

ABS. (2012) Older Carers. 4102.0 - Australian Social Trends. Australian Bureau of Statistics.

ABS. (2015) Get Ready to get digital with the 2016 Census. Media Release, Retrieved 10th September: http://www.abs.gov.au/ausstats/abs@.nsf/mediareleasesbyReleaseDate/EC8D47BE72A97E7 ECA257E9A00131583?OpenDocument

ABS. (2017) Australian Marriage Law Postal Survey, Retrieved on October 29th 2017 from: http://www.abs.gov.au/ausstats/abs@.nsf/mf/1800.0

ACCAN, (2010) Peak communications body says set-top box scheme is essential, Australian Communications Consumer Action Network, retrieved April 22nd 2015 from https://accan.org.au/news-items/media-releases/316-peak-communications-body-says-set-top-box-scheme-is-essential-and-sound

ACMA. (2009). Australia in the Digital Economy series: Report 1 Trust and Confidence *Australian Communications and Media Authority*. Canberra.

ACMA, (2012) Microsoft imposters' phone scam. My Online World, Staying Safe online: Australian Communications and Media Authority, Retrieved February 2015 from http://www.acma.gov.au/Citizen/Stay-protected/My-online-world/Staying-safe-online/qa-microsoft-imposters-phone-scam-i-acma

Advocacy and Rights Centre (2008) Discrimination in the provision of banking and financial services to older people, November 2008 Supplement. Retrieved 8th of March 2013 from http://www.google.com.au/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8 &ved=0CCMQFjAB&url=http%3A%2F%2Flcclc.org.au%2Fwp-content%2Fuploads%2F2012%2F02%2FDiscrimination-Supplement.pdf&ei=xwtcVciuJ9bW8gXp8IGgAw&usg=AFQjCNGEp7V3f_tLAmAe0C4Y U-NUywp1LA

Agarwal, R, Ahuja, M, Carter, P.E., & Gans, M. (1998). *Early and Late Adopters of IT Innovations: Extensions to Innovation Diffusion Theory*. Paper presented at the Proceedings of the DIGIT Conference.

Agarwal, R, Animesh, A., & Prasad, J. (2009). Social Interactions and the "Digital Divide": Explaining Variations in Internet Use. *Information Systems Research, 20*(2), 277 - 294. doi: 10.1287/isre.1080.0194

Agarwal, R, & Prasad, J. (1997). The role of innovation characteristics and perceived voluntariness in the acceptance of information technologies. *Decision Sciences, 28*(3), 557 – 582

Agich, G. (2003) *Dependence and autonomy in old age: An ethical framework for long-term care.* Cambridge. Cambridge University Press.

Ahmed, A. (1966). On the Theory of Induced Innovation. *Economic Journal, 76*, 344 - 357.

AHRC. (2012). Inquiry into Cybersafety for Senior Australians *Ausralian Human Rights Commission Submission to the Joint Select Committee on Cybersafety.* Pitt Street Sydney: Australian Human Rights Commission.

Ajzen, I., and Fishbein, M. (1980) *Understanding Attitudes and Predicting Social Behaviour.* Prentice-Hall, Englewood Cliffs, New Jersey.

Ajzen, I. (1985). From intentions to actions: A theory of planned behaviour. In J. Kuhl & J. Beckmann (Eds.), *Action Control: From cognition to behaviour* (pp. pp. 11 - 39). New York: Springer-Verlag.

Ajzen, I. (1991). The theory of planned behaviour. *Organized Behaviour and Human Decision Processes, 50*, 179 - 211.

Alawadhi, S., & Morris, A. (2008, 7-10 Jan. 2008). *The Use of the UTAUT Model in the Adoption of E-governmnet Services in Kuwait.* Paper presented at the The 41st Hawaii International Conference on System Sciences, Waikoloa, HI

Alawadhi, S., and Morris, S. (2009) factors Influencing the Adoption of E-government Services, *Journal of Software,* Vol 4, No 6. pp 584 – 590.

Alcalde, B., Dubois, D., Mauw, S. Mayer, N. and Radomirovic, S. (2009). Towards a decision model based on trust and security risk management. In *ASIC 2009*, Volume 98. Australian Computer Society.

Almenarez, F., Marin, A., Diaz, D, and Sanchez, J. (2006) Developing a model for trust management in pervasive devices, *Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops*, 2006, Retrieved Feb 15th 2015 http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1598984&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D1598984

Alpass, F.M., and Neville, S. (2003) Loneliness, health and depression in older males. *Aging and Mental Health*, Volume 7, pp 212 – 216.

Alsajjan, B., and Dennis, C. (2010) Internet Banking Acceptance Model: Cross-Market examination, *Journal of Business Research*, Volume 63,

Alston, F. (2014) *Culture and Trust in Technology-Driven Organizations*, CRC Press, Boca Raton

Alvarez, R.M., and Hall, T.E. (2003) Point Click and Vote: The Future of Internet Voting, Brookings Institute.

Alvarez, M. (2008). Google Flu Trends Tracks Flu outbreaks, Fast. *L'Atelier Disruptive Innovation.* Retrieved from Trends website: http://www.atelier.net/en/trends/articles/google-flu-trends-tracks-flu-outbreaks-fast

Anderson, C. L., & Agarwal, R. (2011). The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. Information Systems Research, 22(3), 469-490.

Anderson, P., and Tushman, M.L., (1991) Managing through cycles of technological change, *Research Technology*, Volume 34, Issue 3.

ANPEA, (2008). Responding to the financial abuse of older people: Understanding the challenges faced by the banking and financial services sector. Australian Network for the Prevention of Elder Abuse, National Report, Retrieved on the 8th of March 2013 from https://www.google.com.au/?gfe_rd=cr&ei=0gdcVYniK8eN8QfrhoCgAQ&gws_rd=ssl#q=online+banking+compliance+seniors+elderly

APSC. (2012). Leading and shaping a unified, high performing APS, Australian Public Service. Retrieved April 22nd, 2013, from http://www.apsc.gov.au/aps-reform/background-and-perspectives/overview

APWG. (2010). Phishing ActivityTrends Report, 2nd Half, 2010, Unifying the Global Response to Cybercrime: Anti-Phishing Working Group.

Arenas-Gaitan, J., and Peral-Peral, B., (2015) Elderly and Internet Banking: An Application of UTAUT2. *Journal of Internet Banking and Commerce*, Volume 20, Issue 1.

Arfi, N., and Agarwal, S. (2013) Assessment of Knowledge of Cybercrime among Elderly Across residence, *International Journal of Innovative Research and Studies* (IJIRS)

Argyris, C. (1991) Teaching smart people how to learn. *Harvard Business Review*, Volume 69, Issue 3. pp 99- 109.

Aronson, W.A. (2007) Social Psychology. 6th Edition. New Jersey: Pearson Education.

ASIC. (2011). Avoiding Scams: Protecting yourself from scams. *ASIC Money Smart website; Australian Securities and Investment Commision.* Retrieved March 15th, 2011, from https://www.moneysmart.gov.au/scams/avoiding-scams

ASIC. (2013). Online and Mobile banking: Managing your bank accounts. Moneysmart, Simple guidance you can trust. *Australian Securities and Investment Commision.* Retrieved 23rd April 2013, from https://www.moneysmart.gov.au/managing-your-money/banking#Online

Askham, J. (1998) Supporting Care-givers of older people: an overview of problems and priorities, *Australian Journal of Ageing,* Volume 17, pp 5 – 7

Atchley, R. C. (1999). *Continuity and Adaptation in Aging: Creating Positive Experiences*. Johns Hopkins University Press

Atkins, L., and Wallace, S. (2012) Qualitative Research in Education, SAGE Publications: London.

ATO. (2013). *Key Superannuation rates and thresholds*. Australian Taxation Office. Retrieved from http://www.ato.gov.au/super/content.aspx?doc=/content/60489.htm&page=9&H9.

Audit Commission, (2004) Assistive Technology: *Independence and Well-being, 2*. Audit Commission Publications, Wetherby, West Yorkshire.

Audunson, R. (2005). the Public Library as a meeting-place in a multicultural and digital context: The necessity of low-intensive meeting places. *The Journal of Documentation, 61*(3), 429 - 441.

Australian Government (2013) *Cybersafety for Seniors: A Worthwhile Journey*, Joint Select Committee on Cyber Safety. (JSCCS). Retrieved December 14th, 2013 from: http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=jscc/senior_australians/report.htm

Australian Government (2015) *Stay Smart on Line*, retrieved September 5th from https://www.staysmartonline.gov.au/

Australian Government (2016) *Review of the events surrounding the 2016 eCensus: Improving institutional cyber security and practices across the Australian Government* – Alistair MacGibbon, Office of the Special Adviser to the Prime Minister on Cyber Security, Department of the Prime minister and Cabinet. 13th October 2016. Retrieved 12th June 2017 from: http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22publications%2Ftabledpapers%2Fa41f4f25-a08e-49a7-9b5f-d2c8af94f5c5%22

Babbie, E. (1990). *Survey Research Methods (2nd Ed.)*. Belmont: CA: Wadsworth.

Bagozzi, R. P. (2007). The Legacy of the Technology Acceptance Model and a Proposal for a Paradigm Shift. *Journal of the Association for Information Systems, 8*(4), 243-254.

Bagozzi, R. P., & Lee, K-H. (1999). Comsumer Acceptance of and Resistance to Innovations: Decision Making and Implementation Processes. *Advances in Consumer Research, 26*, 218 - 225.

Bai, G., & Y., Guo. (2010). *Activity Theory Ontology for Knowledge Sharing in E-health*. Paper presented at the International Forum on Information Technology and Applications, IFITA, Kunming. Retrieved August 8th 2015 from: http://www.bth.se/fou/forskinfo.nsf/0/d048bb261571bac6c12577dc00621817/$file/IFITA%202010%20submission%20+%20Guohua%20Bai.pdf

Baker, S., Warburton, J., Hodgkin, S., and Pascal, J. (2014) Reimagining the Relationship between Social Work and Information Communication Technology in the Network Society, *Australian Social Work*, Volume 67, Issue 4.

Baltes, P., & Smith, J. (2003). New frontiers in the future of aging: From successful aging of the young old to the dilemmas of the fourth age. *Gerontology*, Volume 49, Issue 2, pp 123 – 135.

Bandura, A. (1982). Self-Efficacy Mechanism in Human Agency. *American Psychologist, 37*, pp. 122 - 147.

Bannister, F., and Connolly, R. (2012) Defining E-Governance. *E-Service Journal,* Volume 8, Issue 2, pp 3 – 25.

Banyte, J., & Salikaite, R., (2008) Economics of Engineering Decisions No. 1, 56 , In *Engineering Economics*, 2008. Retrieved May 12th 2015 from: file:///C:/Users/David/Downloads/11660-33572-1-PB.pdf\

Barker, (2000). *Computing for the mortally terrified and other fantastic futures.* Paper presented at the 2000 Fullbright Symposium: *Implications for an Ageing Population,* Perth, Western Australia.

Barker, (2012). A Generational Comparison of Social Networking Site Use: The Influence of Age and Social Identity. *The International Journal of Aging and Human Development, 74*(2), 163 - 187.

Bednall, J. (2006). Epoche and bracketing within the phenomenological paradigm. *Issues In Educational Research,* 16(2), 123-138.

Belanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *The Journal of Strategic Information Systems,* Volume 17(2), 165-176. doi: Retrieved 18th July from: http://dx.doi.org/10.1016/j.jsis.2007.12.002

Belanger, F., & Hiller, J. S. (2006). A framework for e-government: privacy implications. *Business Process Management Journal, 12*(1), 48-60.

Beldad, A., De Jong, M., and Steehouder, M. (2010) How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust, *Computers in Human Behavior*, Volume 26, pp 857 – 869.

Bell, W. (2011) Foundations of Future Studies: Human Science for a New Era: Values, Objectivity, and the Good Society, Volume 2, Transaction Publishers, New Brunswick.

Benamati, J. (2007). "Trust and distrust in online banking: Their role in developing countries". *Information technology for development (0268-1102)*, Vol 13 (2), p. 161. DOI: 10.1002/itdj.20059

Benamati, J., and Serva, M. A., (2007) Trust and distrust in online banking: Their role in developing countries. Information Technology for Development, Vol 13, Issue 2 pp 161 - 175

Bentler, P. M., & Speckart, G. (1979). Models of attitude-behaviour relations. *Psychological Review, 86*, 425 - 464.

Berrelez, R. (2000). *Fraud against Seniors, A Prepared statement of the Federal Trade Commission*. Indianapolis, Indiana: Retrieved from http://www.ftc.gov/os/2000/08/agingtestimony.htm.

Berk, L.E. (2010) *Development through the lifespan*, 5th Edition, Boston, Massachusetts: Allyn and Bacon.

Bernard, H.R. (2000). *Social Research Methods: Qualitative and quantitative approaches*. Thousand Oaks, CA: SAGE

Bernard, H.R. (2002). Research Methods in Anthropology: Qualitative and quantitative methods. 3rd edition. AltaMira Press ,Walnut Creek, California.

Bevir, M. (2009) *Key Concepts in Governance*. London: SAGE Publications.

Bhat, H. (2012) An Empirical Study on Usages of Electronic Banking Products and Services in Delhi-NCR with special reference to Senior Citizens, International Management Institute International Conference on Banking and Finance, New Delhi 2012.

Bhattacherjee, A., and Sanford, C. (2006) Influence Processes for Information Technology Acceptance: An Elaboration Likelihood Model, *MIS Quarterly*, Vol. 30, No. 4, pp. 805-825

Bitterman, N., & Shalev, I. (2004). The Silver Surfer: Making the Internet Usable for Seniors. *Ergonomics in Design: The Quarterly of Human Factors Applications, 12*(1), 24-28. doi: 10.1177/106480460401200107

Bizrate, (2000). Survey: 75% of Online Consumers Abandon Shopping Carts without completing a purchase. Retrieved May 25th, 2013, from: http://www.internetnews.com/ec-news/article.php/228561/Survey+75+of+Online+Consumers+Abandon+Shopping+Carts.htm

Blackledge, D., and Hunt, B. (1985). Sociological interpretations of education. London: Routledge.

Blake, M. (1998). Internet Access for older people. *Aslib Proceedings, 50*(10), 308 - 315. doi: 10.1108/eb051509

Blanton, K. (2012) The Rise of Financial Fraud: Scams Never Change but disguises do. *The Center for Retirement Research, Boston College, Working Paper.* Retrieved 14th March 2015 from http://crr.bc.edu/wp-content/uploads/2012/03/Scams-RFTF.pdf

Blythe, J., Camp, J., and Garg, V. (2011) Targeted Risk Communication for Computer Security, Proceedings of the 16th International Conference on Intelligent User interfaces, ACM, pp 295 – 298

Boase, J., Horrigan, J.B., Wellman, B., and Rainie, L. (2006) The Strength of internet ties, Washington, DC: Pew Internet and American Life Project. Retrieved 3rd March 2015 from http://www.pewinternet.org/pdfs/PIP_Internet_ties.pdf

Bordia, S. (2009). How may I be of Service? Foreign Accent Adoption in Off-Shore Call Centres, In the *Proceedings of the Annual Conference of the Australian and New Zealand Academy of Management* (ANZAM 2009) Retrieved 30th January 2016 from https://digitalcollections.anu.edu.au/handle/1885/38062

Bosler, A.M., and Holt, T.J. (2009) Online activities, guardianship, and malware infection: An examination of Routine Activities Theory, *International Journal of Cyber Criminology,* Volume 3, Issue 1, pp 400 – 420.

Botella, C., Etchemendy, E., Castilla, D., Banos, R.M., Garcia-Palacios, A., Quero, S., Alcaniz, M., and Lozano, J.A., (2009) An e-Health System for the Elderly (Butler Project): A Pilot Study on Acceptance and Satisfaction, *Cyber Psychology & Behaviour,* Volume 12, Number 3. Retrieved May11th 2014 from: https://www.researchgate.net/profile/Cristina_Botella/publication/24430604_An_e-Health_System_for_the_Elderly_%28Butler_Project%29_A_Pilot_Study_on_Acceptance_and_Satisfaction/links/0912f50826d21c727b000000.pdf

Boulton-Lewis, G. M. (2010). Education and Learning for the Elderly: Why, How, What. *Educational Gerontology, 36* (3), 213-228. doi: 10.1080/03601270903182877

Bouma, H., Fozard, J.L., Bouwhuis, D.G., and Taipale, V.T. (2007) Gerontechnology in Perspective, Gerontechnology, Volume 6, No 4. Pp 190 – 216

Bradley, N., and Poppen, W. (2003) Assistive technology, computers and internet may decrease sense of isolation for homebound elderly and disabled persons. *Technology and Disability*, Volume 15. pp19 – 25.

Brass, M. and Haggard, P. (2007). To do or not to do: the neural signature of self-control. *Journal of Neurosci,* Volume 27, pp 9141 – 9145.

Bratkiewicz, J. L. (2000). Here's a Quarter, Call Someone Who Cares: Who Is Answering the Elderly's Call for Protection from Telemarketing Fraud. *South Dakota Law Review, 45*.

Bright, A.K., and Coventry, L. (2013) Assistive technology for older adults: psychological and socio-emotional design requirements, *Proceedings of the 6th International Conference on Pervasive Technologies related to assistive environments,* Article 9, ACM.

Brown, S.A., Massey, A.P., Montoyo-Weiss, M.M., and Burkman, J.R., (2002) Di I really have to? User acceptance of mandated technology, *European Journal of Information Systems*, Volume 11, pp 283 – 295.

Brown, S.A., Dennis, A.R. and Venkatesh, V. (2010) Predicting Collaboration Technology Use: Integrating Technology Adoption and Collaboration Research, *Journal of Management Information Systems*, Volume 27, Issue 2. pp 9 – 54.

Browne, R. (2014) Blind Woman Gisele Mesnage sues Coles over online shopping website, *The Sydney Morning Herald*, November 5th 2014, Retrieved August 14th 2016 from: http://www.smh.com.au/digital-life/digital-life-news/blind-woman-gisele-mesnage-sues-coles-over-online-shopping-website-20141105-11h6zw.html

Browne, S., Lang, M., and Golden, W. (2014) Threat avoidance and security adoption: A theoretical model for SMEs, *Proceedings of 2014 IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop.*

Bruder, C., Blessing, L, and Wandke, H. (2014) Adaptive Training Interfaces for Less-Experienced, Elderly Users of Electronic Devices, *Behavioural Information Technology*, Volume 33, Issue 1, pp 4 – 15.

Brush, C.G., Edelman, I.F., and Manolova, T.S. (2011)Initial Resource Assembly in New Ventures: Does Location matter? In *Psicothema*, Volume 23, Issue 3, pp 439-445

Burmeister, O. (2010) Virtuality Improves the Well being of Seniors through increasing social Interaction, J.Berleur et al. (Eds) : HCC9/CIP 2010. IFIP AICT 328, pp131 – 141

Byner, L. (2016) Traps for anyone completing their Census online: *News, FiveAA* August 8th 2016. Retrieved on October the 18th from: http://www.fiveaa.com.au/shows/leon-byner/trap-for-anyone-completing-their-census-online

Byrne, G.J., & Staehr, L.J. (2006). *Current Internet Use in Australia: A Closer Look at the Digital Divide.* Paper presented at the ACIS 2006 proceedings.

Cameron, D., Marquis, R., and Webster, B. (2001) Older adults' perceptions, experiences and anxieties with emerging technologies, *Australasian Journal of Ageing*, Volume 20, Issue 2, pp 50 – 56

Campbell, R., Carter, L., Hobbs, J., & Schaupp, L. C. (2012). E-government utilization: understanding the impact of reputation and risk. *International Journal of Electronic Government Research, 8*, 83+.

Campbell, D., and Frei, F. (2010) Cost Structure, Customer Profitability, and Retention Implications of Self-Service Distribution Channels: Evidence from Customer Behavior in an Online Banking Channel. *Management Science*, Vol 56(1): pp 4-24. Retrieved September 29th, 2014 from: http://dx.doi.org/10.1287/mnsc.1090.1066

Campbell, R.J., and Wabb, J. (2003). The elderly and the internet: A case study. *Internet Journal of Health.* Volume 3, Issue 1, pp 2 – 15.

Canton, E.J.F., de Groot, H.L.F., and Nahuis, R. (2002) Vested Interests, populations ageing and technology adoption. *European Journal of Political Economy*, Volume 18, Issue 4. pp 631 – 652.

Caplan, S.E., (2007) Relations among loneliness, social anxiety, and Problematic Internet use. *Cyberpsychology and Behaviour.* Volume 10, issue 2. pp234 – 242.

Caprani, N., Doyle, J., O'Grady, M., Gurrin, C., O'Connor, N., Caufield, B., and O'Hare,G., (2012) Technology use in everyday life: Implications for designing for older users. Technology use in everyday life: Implications for designing for older users. In: *iHCI 2012: 6th Annual Irish Human Computer Interaction* (HCI) Conference, 20-21 June 2012, Galway, Ireland

Carlson, E.L. (2006) Phishing for Elderly Victims: As the Elderly Migrate to the Internet Fraudulent Schemes Targeting Them Follow, *Elder Law journal,* Volume 14. pp 423 – 452

Carlsson, B., Jacobsson, S., Holmen, M., and Rickne, A. (2002) Innovation systems: analytical and methodological issues, *Research Policy*, Volume 31, pp 233 – 245.

Carlton, N., Fear, T., and Means, R. (2004) Responding to the Harassment and Abuse of Older People in the Private Rented Sector: Legal and Social Perspectives. *Journal of Social Welfare and Family Law.* Volume 26, Issue 2, pp 131 – 145.

Carmichael, A., Rice, M., Sloan, D., and Gregor, P. (2006) Digital switchover or digital divide: a prognosis for usable and accessible interactive digital televisoin in the UK, *Universal Access in the Information Society*, Volume 4, pp 400-416 DOI: 10.1007/s10209-005-0004-x

Chaiken, S. (1980) Heuristic versus systematic processing in the use of source versus message cues in persuasion, *Journal of Personality and Social Psychology*, Volume 39, pp 752 – 766

Chakraborthy, R., Bagchi-Sen, S., Rao, R.H., and Upadhyaya, S. (2012). An exploration of security and Privacy behaviour of Elders on the Internet and Comparison with Younger Adults. *Proceedings of the Seventh Pre-ICIS Workshop on Information Security and Privacy*, Orlando, December 15, 2012.

Chakraborthy, R., R., Rao., Sankaranarayanan, V., & Upadhyaya, S. (2008). *Mediated Internet Experience for Senior Citizens.* Paper presented at the AMCIS 2008 Proceedings.

Chan, F. K. Y., Thong, J. Y. L., Venkatesh, V., Brown, S. A., Hu, P. J. H., & Tam, K. Y. (2010). Modeling Citizen Satisfaction with Mandatory Adoption of an E-Government Technology. *Journal of the Association for Information Systems, 11*(10), 519 - 549.

Chang, B. L. (1979) Locus of control, trust, situational control and morale of the elderly, *International Journal of Nursing Studies*, Volume 16, pp 169 – 181. Pergamon Press Limited.

Chang, J., McAllister, C., and McCaslin, R. (2015) Correlates of, and Barriers to, Internet Use Among Older Adults. *Journal of Gerontological Social Work*, Volume 58, Issue 1. pp 66-85

Charmaz, K. (2006) *Constructing Grounded Theory: A Practical Guide through Qualitative Research.* Sage Publications Ltd: London

Charness, N. (2004). Preface. In D. C. Burdick & S. Kwon (Eds.), *Gerontechnology: research and practice in technology and aging* (pp. xxv - xxvii). New York: Springer.

Charness, N., & Boot, W. R. (2009). Aging and Information Technology Use: Potential and Barriers. *Current Directions in Psychological Science, 18*(5), 253-258. doi: 10.1111/j.1467-8721.2009.01647.x

Chattaraman, V., Kwon, W., and Gilbert, J.E. (2012) Virtual agents in retail web sites: Benefits of simulated social interaction for older users. *Computers in Human Behaviour*, Volume 28, Issue 6, pp 2055 – 2066.

Chawki, M. (2009). Nigeria Tackles Advance Fee fraud. *Journal of Information, Law, &Technology, 1*.

Checkland, P., and Poulter, J. (2010) Soft Systems Methodology, in Martin Reynolds and Sue Holwell (Eds) *Systems Approaches to Managing Change: A Practical Guide*, pp 191 – 241.

Chen, L.D., Gillenson, M.L., and Sherell, D.L. (2002) Enticing online consumers: an extended technology acceptance perspective. *Information and Management*, Volume 39, Issue 8. pp 705 – 719.

Chen, P., and Hitt, L.M. (2002) Measuring switching costs and the determinants of customer retention in internet-enabled businesses. A study of the online brokerage industry. *Information Systems Research*, Volume 13, pp 255 – 274.

Chen, S., & Li, S. (2010). Consumer adoption of e-service: Integrating technology readiness with the theory of planned behavior. *African Journal of Business Management, 4*(16), 3556-3563.

Chesbrough, H., and Crowther, A.K., (2006). Beyond high tech: early adopters of open innovation in other industries. *R&D Management*, Volume 36, Issue 3.

Chesters, J, Ryan, C, & Sinning, M. (2013). *Older Australians and the take-up of new technologies*. Canberra: National Vocational Education and Training Research Program NCVER.

Chong, A. Y., Keng-Boon, O, Lin, B., and Tan, B. (2010). "Online banking adoption: an empirical analysis". *International journal of bank marketing (0265-2323)*, 28 (4), p. 267. DOI: 10.1108/02652321011054963

Choo, K.K.R., (2011) The Cyber threat landscape: Challenges and future research directions, *Computers and Security*, Vol 30 pp 719 – 731

Christ, J. D., and Tanner, C. A. (2003). Interpretation/analysis methods in hermeneutic interpretive phenomenology. *Nursing Research*, Volume 52, Issue 3.

Chu, A., Huber, J., Mastel-Smith, B., and Cesario, S. (2008) Partnering with Seniors for Better Health: computer use and Internet health information retrieval among older adults in a low socio-economic community, *Journal of the Medical Library Association*, Volume 97, Issue 1, pp 12 – 20.

Chuttur, M. (2009). Overview of the Technology Acceptance Model: Origins, Developments and Future Directions *Sprouts: Working papers on Information Systems* (Vol. 9). Indiana University USA.

Citibank. (2013). e-Statements: Online and Mobile banking, Citibank Australia. Retrieved March 13, 2013, from http://citibank.com.au/aus/banking/banking_internetbanking.htm

Citibank. (2016) History of Citibank in Australia. Landmark Events. Retrieved August 14th 2016 from: https://www.citibank.com.au/aus/static/aboutus_history.htm

Clare, M., Blundell, B., Clare, J. (2011) Examination of the Extent of Elder Abuse in Western Australia: A Qualitative and Quantitative Investigation of Existing Agency Policy. In: Service Responses and Recorded Data. Crime Research Centre, the University of Western Australia

Cleveland, S., (2012) In search of user privacy protection in ubiquitous computing, *2012 IEEE International Conference on Information Reuse and Integration.* Retrieved January 2015 from: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6303077&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6303077

Clothier, R.A., Greer, D.A., Greer. D.G., and Mehta, A.M. (2015) Risk Perception and the Public Acceptance of Drones. Risk Analysis: Wiley Online Library, Retrieved February 10th 2015,.https://www.researchgate.net/profile/Reece_Clothier/publication/272420649_Risk_Perception_And_The_Public_Acceptance_Of_Drones/links/5580b68308ae607ddc3227d3.pdf

Cohen, A. (2001). Internet insecurity. Time, 157(26), 44-51

Cohen, C., (2006) Consumer Fraud and the Elderly: A review of Canadian Challenges and Initiatives, *Journal of Gerontological Socialwork*, Volume 46, Issue 3-4, pp 137-144.

Cohen, L., Manion, L., & Morrison, K. (2008). *Research Methods in Education (6th Ed.).* Oxford, UK: Routledge.

ComLaw. (2004). *Age Discrimination Act 2004*. Australian Government. Retrieved from http://www.comlaw.gov.au/Details/C2012C00907/Download.

Conci, M., Pianesi, F., Zancanaro, M. (2009) Useful, social and enjoyable: Mobile phone adoption by older people. In *INTERACT, Part 1*. T Gross et al (Eds): LNCS 5726 IFIP International Federation for Information Processing.

Consumer Affairs. (2016) Customer Complaints and Reviews: Citibank. Retrieved 5th September 2016 from: https://www.consumeraffairs.com/finance/citibank.htm

Conway, V. (2014) Website Accessibility in Australia and the National Transition Strategy: Outcomes and Findings, Doctoral Thesis, Edith Cowan University, Retrieved on 4th March 2015 at http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=2406&context=theses

Cook, D. M., Szewczyk, P. S., & Sansurooah, K. (2011a). Securing the Elderly: A Developmental Approach to Hypermedia-Based Online Information Security for Senior Novice Computer Users. Paper presented at the *Proceedings of the 2nd International Cyber Resilience Conference,* Perth, Western Australian.

Cook, D. M., Szewczyk, P. S., & Sansurooah, K. (2011b). Seniors Language Paradigms: 21st Century Jargon and the Impact on Computer Security and Financial Transactions for Senior Citizens. *Proceedings of the 9th Australian Information Security Management Conference.* Paper presented at the Australian Information Security Management Conference, Perth, Western Australia.

Cook, E.J., Randhawa, G., large, S., Guppy, Chater, and Ali, (2014) Barriers and Facilitators to using NHS Direct: a qualitative study of "users" and "non-users". *BMC Health Services Research*, Volume 14, p487, Retrieved 12 March 2015 from http://www.biomedcentral.com/1472-6963/14/487

Cooper, R. B., & Zmud, R.W. (1990). Information Technology Implementation Research: A Technological Diffusion Approach. *Management Science, 36*(2 (Feb)), 123 - 139.

Coronges, K., Dodge, Ronald, Mukina, C., Radwick, Z., Shevchik, J., & Rovira, E. (2012, 4-7 Jan. 2012). *The Influences of Social Networks on Phishing Vulnerability*. Paper presented at the System Science (HICSS), 2012 45th Hawaii International Conference on.

Cortes, U., Annicchiarico, R., Vázquez-Salceda, J., Urdiales, C., Cañamero, L., López, M., . . . Caltagirone, C. (2003). Assistive technologies for the disabled and for the new generation of senior citizens: the e-Tools architecture. *AI Communications, 16*(3), 193-207.

Cortes, U., Barrue, C., Martinez, A. B., Urdiales, C., Campana, F., Annicchiarico, R., & Caltagirone, C. (2010). Assistive technologies for the new generation of senior citizens: the SHARE-it approach. *International Journal of Computers in Healthcare, 1*(1), 35-65. doi: 10.1504/IJCIH.2010.03413

Cotton, S.R., Anderson, W., and McCullough, B., (2012). The impact of ICT use on loneliness and contact with others among older adults. *Gerontechnology*, 2012 Volume 11, Issue2, p161.

Crane, P. R. (2006) Action Research in Social Programs. In *Action Learning, Action Research and Process Management Conversation*, 17th August 2006, Brisbane.

Cresci, M.K., Yarandi, H., and Morrell, R. (2010) The Digital Divide and Urban Adults. *Computers, Informatics, Nursing,* Volume 28, Issue 2, pp 88 - 94

Creswell, J.W. (2009). *Research Design: Qualitative, Quantitative, and Mixed methods Approaches (3rd Edition)* (3rd ed.). Los Angeles: SAGE.

Cresswell, J.W., & Piano Clark, V. L. (2011). *Designing and conducting Mixed Methods Research (2nd Ed.)*. Thousand Oaks: CA: Sage.

CRFB. (1988). *Constitution of the Federative Republic of Brazil*. Brazil: Retrieved from http://www.v-brazil.com/government/laws/constitution.html.

Cruz, P., Laukkanen, T., and Munoz, P. (2011), Exploring the Factors Behind the Resistance to Mobile Banking in Portugal. *International Journal of E-services and Mobile Applications*.

Cumming, E., and Henry, W. E. H. (1961) *Growing Old*. New York: Basic.

Curran, J. M, and Meuter, M. L. (2005). Self-service technology adoption: comparing three technologies. *Journal of Services Marketing,* Volume 19, Issue 2, pp103−113.

Cutler, S.J. (2011) Technological Change and Aging, in the *Handbook of Aging and the Social Sciences*, 6th Edition, Robert H. Binstock, Linda K. George, Stephen J. Cutler, Jon Hendricks, and James H. Schulz (Eds), Academic Press, London.

Cyber-Safety, Parliamentary Joint Select Committee on. (2013). *Cybersafety for Seniors: A Worthwhile Journey*: Australian Government - Department of the House of Representatives.

Cymek, D. H., Burglen, J. and Minge, M. (2014) Identifying the potential to motivate older adults' use of information and communication technology through serious games. *1st international Symposium on Simulation & Serious Games* (ISSSG 2014)

Czaja, S. J., & Hiltz, S. R. (2005). Digital Aids for an Aging Society. *Communications of the ACM,* Volume 48, Issue 10, 43–44.

Czaja, S.J., & Lee, C.C. (2007). The impact of aging on access to technology. *Universal Access in the Information Society, 5*(4), 341-349. doi: 10.1007/s10209-006-0060-x

Dalcher, I. And Shine, J. (2003) Extending the New Technology Acceptance Model to Measure the End User Information Systems satisfaction in a Mandatory Environment: A Bank's Treasury. *Technology Analysis and Strategic Management*, Volume 15, Issue 4. pp441 – 455.

Dannefer, D. (1987). Aging as intracohort differentiation: Accentuation, the matthew effect and the life course. *Sociological Forum, 2*, 211-236.

Dannefer, D. (2003). Cumulative Advantage / Disadvantage and the Life Course: XCross Fertilizing Age and Social Science Theory. *The Journals of Gerontology, Series B, Volume 58* (6).

Davies, M.L., Gilhooly, M.L.M., Gilhooly, K.J., Harries, P.A., and Cairns, D. (2013). Factors influencing decision-making by social care and health sector professionals in cases of elder financial abuse.

Davis, F. D. (1986). *A Technology Acceptance Model for Empirically testing New End-User Information Systems: Theory and Results.* (Doctoral Dissertation), Massachusetts Institute of Technology, Massachusetts

Davis, F. D. (1989) Perceived usefulness, perceived ease of use and user acceptance of information technology. *MIS Quarterly,* Volume 13, Issue 3, pp 319 – 339.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science, 35*(8), 982-1003. doi: 10.2307/2632151

DBCDE. (2012). Review of access to telecommunication services by people with disability, older Australians and people experiencing illness, Department of Broadband, Communications and the Digital Economy: Australian Government.

Deimann, M., & Bastiaens, T. (2010). The role of volition in distance education: An exploration of its capacities. *The International Review of Research In Open And Distributed Learning, 11*(1), 1-16. Retrieved from http://www.irrodl.org/index.php/irrodl/article/view/778/1484

Dekimpe, M.G., Parker, P.M., and Sarvary, M. (2000) Global diffusion of technological innovations: a coupled-hazard approach, Journal of Marketing Research, Volume 37, Issue 1. pp47-59

De Koning, J. and Gelderblom, A. (2006) ICT and Older Workers: no unwrinkled relationship. *International Journal of Manpower*, Volume 27, No. 5.

Dekker, s., (2014). *The field guide to understanding 'Human Error'*, Ashgate Publishing; Hampshire

Denscombe, M. (2010) Good Research Guide: For small-scale social research projects (4th Edition). Open University Press. Berkshire, Great Britain.

Denzin, N. And Lincoln, Y. (Eds). (1998). *Handbook of Qualitative Research*. Thousand Oaks: Sage Publications.

DHA. (2013). PCEHR National Health Reform, Department of Health and Ageing. (DHA) Retrieved April 12th, 2013, from: http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/Content/110590ACF23D9421CA2 57A330038E881/$File/Consumer-FAQs-for-ehealth-App.pdf

Dhillon, S. K. (2011). ICT Evaluation for Knowledge Sharing among Senior Citizens Community. In J. Mohamad Zain, W. Wan Mohd & E. El-Qawasmeh (Eds.), *Software Engineering and Computer Systems* (Vol. 179, pp. 92-103): Springer Berlin Heidelberg.

DHS. (2012). Changes to the Centrelink Statement, Department of Human Services. *Australian Government.* Retrieved April 12, 2012, from

http://www.centrelink.gov.au/internet/internet.nsf/individuals/changes_centrelink_statement.htm

DHS. (2013). *Age pension and planning your retirement*. Department of Human Services. Canberra: Retrieved from http://www.humanservices.gov.au/customer/subjects/age-pension-and-planning-your-retirement.

Diako, B., Lubbe, S., & Klopper, R. (2012). The Degree of Readiness of South African Senior Citizens for Electronic Banking: An Exploratory Investigation. *Alternation Journal,* (Emerging Trends in Management, Informatics and Communication in a Digitally Connected World), 255 - 287.

Dick, B., Passfield, R., and Wildman, P. (1995) Action research for beginners. ARCS Newsletter, 3(1) pp 3 – 6. Retrieved December 7th 2015 from www.aral.com.au

Dick, B. (1999). What is action research? Retrieved December 15th 2015 from: http://www.scu.edu.au/schools/gcm/ar/arp/arfaq.html

Dickinson, A., Arnott, J., & Prior, S. (2007) Methods for human-computer interaction research with older people. *Behaviour & Information Technology,* Vol.26, No.4, July-August 2007, pp.343-352. http://www.informaworld.com/openurl?genre=article&issn=0144-929X&volume=26&issue=4&spage=343

Dickinson, A., Smith, M.J., Arnott, J.L., Newell, A.F., and Hill, R.L. (2007) Approaches to Web Search and Navigation for Older Computer Novices. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. San Jose, California.

Dijkstra, J.J. (1999) User agreement with incorrect expert system advice, *Behaviour and Information Technology,* Volume 18, Issue 6, pp 399 – 411.

Diniz, E., Birochi, R., and Pozzebon, M. (2012) Triggers and barriers to financial inclusion: The use of ICT-based branchless banking in an Amazon county, *Electronic Commerce, Research, and Applications.* Volume 11, Issue 5, pp 484 – 494

DiPrete, T., & Eirich, G. M. (2005). Cumulative Advantage as a Mechanism for Inequality: A Review of Theoretical and Empirical Developments. *Annual Review of Sociology, 32*, 271-297.

Dishaw, M. T., & Strong, D. M. (1999). Extending the technology acceptance model with task-technology fit constructs. *Information and Management, 36*, 9 - 21.

Dormann, W., and Rafail, J. (2006) Securing Your Web browser, Software Engineering Institute, Carnegie Mellon, Retrieved 12th March 2015, from http://www.alkalbany.net/documents/NETW4005-Lab1.pdf

Duggan, M, and Smith, A., (2013) Demographics of key social networking platforms, Pew Research Center: Internet, Science and Tech. Retrieved October 8th 2014 from: http://www.pewinternet.org/2013/12/30/demographics-of-key-social-networking-platforms/

Durkin, M., Howcroft, B., O'Donnell, A. and McCartan-Quinn, D. (2003). "Retail bank customer preferences: personal and remote interactions". *International journal of retail & distribution management (0959-0552)*, 31 (4), p. 177.

Durkin, M. (2007). Understanding registration influences for electronic banking. *The International Review of Retail, Distribution and Consumer Research*, Vol 17, pp219 – 231.

Dwyer, P. (2008). The Conditional Welfare State, in *Modernising the Welfare State* (ed., Powell, M.) Policy Press, Bristol.

Dyer, C.B., Heisler, C.J., Hill, C.A. and Kim, L.C. (2005). Community Approaches to Elder Abuse, *Clinics in Geriatric Medicine*, Volume 21, pp 429-447.

Dyson, L.E. (2003) Indigenous Australians in the Information Age: Exploring Issues of Neutrality in Information Technology, Indigenous Australians in the Information Age, in Ciborra, C., Mercurio, R., De Marco, M., Martinez, M. & Carignani, A. (eds.) *New Paradigms in Organizations, Markets and Society: Proceedings of the 11th European Conference on Information Systems* (ECIS), Naples, Italy, 19 – 21 June 2003.

Eastman, J., and Iyer, R. (2004). The elderly's uses and attitudes towards the Internet. *The Journal of Consumer Marketing,* Volume 21(2/3), 208-220.

Eggermont, S., Vandebosch, H., & Steyaert, S. (2006). Towards the desired future of the elderly and ICT: policy recommendations based on a dialogue with senior citizens. *Poiesis & Praxis, 4*(3), 199-217. doi: 10.1007/s10202-005-0017-9

Eisma, R., Dickinson, J., Goodman, A, Syme, L., Tiwari, and Newell, (2004) Early user involvement in the development of information technology-related products for older people. *Universal Access in the Information Society*, Volume 3, Issue 2 pp 131 – 140.

Elder, V., Gardner, E. and Ruth, S. (1987) Gender and age in technostress: effects of white-collar productivity, *Government Finance Review*, Vol. 3 No.6, pp17-21.

Elliott, J. (1991) *Action research for educational change*. Pennsylvania: Open University Press.

Ellis, R. D., & Allaire, J. C. (1999). Modeling computer interest in older adults: The role of age, education, computer knowledge, and computer anxiety. *Human Factors, 41*(3), 345-345.

Elster, J. (1983). *Explaining technical change : a case study in the philosophy of science* Cambridge: Cambridge University Press.

Engestrom, Y. (1987) Learning by Expanding: An Activity-theoretical Approach to Developmental Research. Orienta-Konsultit. ISBN 9519593322

Eriksson, K., Kerem, K., & Nilsson, D. (2005). Customer acceptance of internet banking in Estonia. *International Journal of Bank Marketing, 23*(2).

Fairchild, A. M. (2003, 6-9 Jan. 2003). *Value positions for financial institutions in electronic bill presentment and payment (EBPP).* Paper presented at the System Sciences, 2003. *Proceedings of the 36th Annual Hawaii International Conference on System Sciences.* Retrieved 3rd August 2014 from: http://s3.amazonaws.com/academia.edu.documents/26215532/10.1.1.10.8587.pdf?AWSAccessKeyId=AKIAJ56TQJRTWSMTNPEA&Expires=1479132093&Signature=IsZFcCnnVvJKpfnFSnD%2FEwP2To0%3D&response-content-disposition=inline%3B%20filename%3DValue_Positions_for_Financial_Institutio.pdf

Faletti, M.V., (1985) From Can Openers to Computers: Technology can enhance functional ability and independence for the aged, in *Caring*, January pp56 – 58

Fano, A., & Gershman, A. (2002). The future of business services in the age of ubiquitous computing. *Communication. ACM,* Volume 45, Issue 12, 83-87. doi: 10.1145/585597.585620

Fast, J., Keating, N. C., Derksen, L., & Otfinowski, P. (2004). Characteristics of Family/Friend Care Networks of Frail Seniors. *Canadian Journal of Aging, 23*(1), 5 - 19. doi: 10.1353/cja.2004.0003

FBI, (2006) *Fraud Target: Senior Citizens, Common Fraud Schemes; seniors.* The Federal Bureau of Investigation, (FBI). United States of America. Retrieved February 6th from: http://www.fbi.gov/scams-safety/fraud/seniors/seniors

Fealy, G., Donnelly, N., Bergin, A., Treacy, M.P., Phelan, A. (2012) *Financial Abuse of Older People: A Review*, NCPOP, University College Dublin.

Ferreira, S., Torres, A., Mealha, O., and Veloso, A. (2015) Training Effects on Older Adults in Information and Communications Technologies Considering Psychosocial Variables. *Educational Gerontology,* Vol 41, Issue 7, pp 482 – 493

Festervand, T., Meinert, D.B., and Vitell, S. J. 1994; Older Adults' Attitudes Toward and adoption of personal computers and computer-based lifestyle assistance, *Journal of Applied Business Research* JABR Vol 10, No 2, 1994

Finkelstein, A. (2005). The aggregate effects of health insurance: evidence from the introduction of Medicare, *The National Bureau of Economic Research, NBER Working Paper No. 11619*, (DOI): 10.3386/w11619

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior : an introduction to theory and research*. Reading, Mass.: Addison-Wesley Pub. Co.

Fisher, K., and Phelps, R. (2006) Recipe or performing art? Challenging conventions for writing action research theses, *Action Research*, Volume 4, No. 2, pp 143-164.

Fisk, A.D., Rogers, W.A., Charness, N., Czaja, S.J., & Sharit, J. (2009). *Designing for Older Adults: Principles and Creative Human Factors Approaches* (2nd ed. ed.): Boca Raton : CRC Press, c2009.

Fleeger, C.P., and Fleeger, S.L. (2009) Security in Computing, 6th Edition, Wesford Massachusetts,

Floh, A., and Treiblmaier, H. (2006). What keeps the E-Banking customer loyal? A Multigroup analysis of the moderating role of consumer characteristics on E-loyalty in the Financial Service industry. *Journal of Electronic Commerce Research,* Volume 7, Issue 2

Floyd, S.W., and Shaker, A.Z. (2007) The Effect of fit between competitive strategy and IT adoption on organizational performance in small banks, *Technology Analysis and Strategic Management*, Volume 2 Issue 4. Pp 357 - 372

Forsythe, S.M., and Shi, B. (2003) Consumer patronage and risk perceptions in Internet Shopping, *Journal of Business Research*, Volume 56, pp 867 – 875.

Friemel, T. N. (2014) The Digital divide has grown old: determinants of a digital divide among seniors, *New Media and Society*, 2014. pp 1 – 19.

Frith, C. (2007). Making up the Mind: How the Brain creates our mental world. Blackwell Publishing, Oxford.

Frumento, E., and Freschi, F. (2016) How the Evolution of Workforces Influences Cybercrime Strategies: *The Example of Healthcare, in Combatting Cybercrime and Cyberterrorism,* Babak Akhgar and Ben Brewster (Eds.), Springer International Publishing, Ch 4, pp 237 – 258.

Fuchsberger, V. (2008) Ambient assisted living: elderly people's needs and how to face them. *Proceedings of the 1ˢᵗ ACM international workshop on Semantic ambient media experiences,* pp 21 – 24. Retrieved 23ʳᵈ March 2015 from http://dl.acm.org/citation.cfm?id=1461917

Fujitsu. (2012). Raku-Raku smartphone debut offers easy touch operations on a large-screen display. Retrieved February 12th, 2013, from http://www.fujitsu.com/global/news/pr/archives/month/2012/20120726-01.html

Furnell, S. (2004) E-commerce security: a question of trust. *Computer Fraud and Security*. Volume 2004, Issue 10, pp 10 – 14.

Furnell, S., Bryant, P., and Phippen, A. (2007) Assessing the Security Perceptions of Personal Internet Users, *Computers and Security*, Volume 26, issue 5 pp 410 – 417.

Gagliardi, C., Mazzarini, G., Papa, R., Giuli, C., & Marcellini, F. (2007). Designing a Learning Program to Link Old and Disabled People to Computers. *Educational Gerontology, 34*(1), 15-29. doi: 10.1080/03601270701763902

Gall, M. D., Gall, J. P., & Borg, W. R. (2007). *Educational research: An introduction*. (8th ed.). Boston: Pearson Education, Inc.

Galliers, R.D. and Land, F.F. (1987). Choosing Appropriate Information Systems Research Methodologies. *Communications of the ACM*, Volume 30, Issue no. 11.

Galliers, R.D. (1993). Research Issues in Information Systems, *Journal of Information Technology,* Volume 8, Issue no. 2. pp 92 – 98.

Gambetta, D. (2000) Can We Trust Trust?: in Diego Gambetta (ed.) *Trust: Making and Breaking Cooperative Relations*, Department of Sociology, University of Oxford, Chapter 13, pp 213 – 237. Retrieved 23ʳᵈ April 2015 from http://www.sociology.ox.ac.uk/papers/gambetta213-237.pdf

Gamble, K.J., Boyle, P., Yu, L., and Bennett, D. (2014) The Causes and Consequences of Financial Fraud among older Americans. The Center for Retirement Research, Boston College, Working Paper. Retrieved 14ᵗʰ March 2015 from: http://crr.bc.edu/wp-content/uploads/2014/11/wp_2014-13.pdf

Gan, C, Clemes, M, Limsombunchai, V, & Weng, A. (2006). A logit analysis of electronic banking in New Zealand. *International Journal of Bank marketing, 24*(6), 360 - 383. doi: 10.1108/02652320610701717

Gao, W., & Kim, J. (2007) Robbing the cradle is like taking candy from a baby. Paper presented at *the Annual Conference of the Security Policy Institute*, Amsterdam, the Netherlands.

Gao, J., & Koronios, A. (2010). *Mobile Applications Development for Senior Citizens*. Paper presented at the PACIS 2010: *The 14th Pacific Asia Conference on Information Systems*, Taipei, Taiwan. http://www.pacis-net.org/index.jsp?t=proceeding&y=2010

Garg, V., Camp, L.J., Lorenzen-Huber, L.M., and Connelly, K. (2011) Designing Risk Communication for Older Adults; The Social Impact of Social Computing, *Proceedings of the 2011 Ethicomp,* De Monfort University. Retrieved February 9ᵗʰ 2015 from http://www.cs.indiana.edu/~connelly/Papers/C26_DesigningRiskCommunication.pdf

Gates, M. (1976). Measuring peasant methods to modernization: a projective method, *Current Anthropology,* Volume 17, pp641 – 665.

Gatto, S. L. and Tak, S.L. (2008). "Computer, Internet, and E-mail Use among Older Adults: Benefits and Barriers". *Educational Gerontology (0360-1277)*, Vol 34 (9), p. 800. DOI: 10.1080/03601270802243697

Gefen, D. (2000) E-Commerce: the role of familiarity and trust, *The International Journal of Management Science*. Volume 27 Issue 1 pp 51–90.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in Online Shopping: An Integrated Model. *MIS Quarterly, 27*(1), 51-90. doi: 10.2307/30036519

GEO. Government Equalities Office. (2010). *Equality Act 2010.* United Kingdom: Retrieved from http://www.legislation.gov.uk/ukpga/2010/15/pdfs/ukpga_20100015_en.pdf.

Gergen, K.J. (1999) Taking Social Constructionism Seriously. London: Sage

Gerling, K. M., and Masuch, M. (2011) Exploring the Potential of Gamification among frail elderly Persons. Vancouver, BC, Canada

Gil, H, & Amaro, F. (2010). *Active Ageing and the Role of ICT and Assistive technologies: Reflections and discussion for their use in Portugal.* Paper presented at the International Conference on e-Commerce, e-Administration, e-Society, e-Education, and e-Technology, Macau 25th - 27th January.

Gilly, M.C., and Zeithaml, (1985). The Elderly Consumer and Adoption of Technologies. *Journal of Consumer Research*, Volume 12, Issue 3, pp 353- 357.

Giroux, H.A. (1986). Critical Theory and the Politics of Culture and Voice: Rethinking the Discourse of Educational Research. *Journal of Thought*, Volume 21, Issue No. 3, pp 84 – 105.

Goff, S. (2007). Participatory practices: On bringing our field together, *ALARA Journal*, Volume 12, Issue 2 pp 106 – 126.

Goodhue, D. L., & Thompson, R. L. (1995). Task-Technology Fit and individual performance. *MIS Quarterly, 19*(2), 213 - 236.

Goodman, P. S. (1986). Impact of Task and Technology on Group Performance. In P. S. G. a. Associates (Ed.), *Designing Effective Work Groups* (pp. pages 120 - 167). San Francisco: Jossey-Bass Publishers.

Gottsdanker, R. (1982). Age and Simple Reaction Time. *Journal of Gerontology, 37*(3), 342-348. doi: 10.1093/geronj/37.3.342

Goujon, P. and Flick, C. (2010) Ethical Governance for Emerging ICT: Opening Cognitive Framing and Achieving Reflexivity. J. Berleur et al. (Eds): *HCC9/CIP 2010 IFIP AICT* No.328, pp 98 – 111.

Grabner-Krauter, S., and Faullant, R. (2008) Consumer acceptance of internet banking: the influence of internet trust, International Journal of Bank Marketing, Volume 26, No 7. pp483 – 504

Grbich, C. (1999). *Qualitative Research in Health*. St Leonards, NSW: Allen and Unwin Pty Ltd.

Grgugic, A. (2012) ICT towards elderly independent living, Research and Development Centre, Ericsson Nikola Tesla, accessed 21st march 2016 from http://www.enhems-buildings.fer.hr/_download/repository/A._Grguric,_rad_KDI.pdf

Grimes, G. A., Hough, M. G., Mazur, E., & Signorella, M. L. (2010). Older Adults' Knowledge of Internet Hazards. *Educational Gerontology, 36*(3), 173-192. doi: 10.1080/03601270903183065

Grimsley, M. And Meehan, A. (2007) e-Government information systems: Evaluation-led design for public value and client trust, *European Journal of Information Systems,* Volume 16, pp 134-148.

Grundy, E. (2005) 'Reciprocity in relationships: Socioeconomic and health influences on intergenerational exchanges between Third Age parents and their adult children in Britain'. *The British Journal of Sociology*, 56 (2), pp 233–255.

Grundy, S. (1987). *Curriculum: Product or Praxis*. Lewes, Palmer

Grundy, S. (1995) Action Research as a Professional Development. *The Big Link Occasional Paper* Volume 1, pp 5 – 22.

Gu, J., Lee, S., and Suh, Y. (2009) Determinants of behavioural intention to mobile banking, *Expert Systems with Applications,* Volume 36, Issue 9. pp 11605 – 11616

Guba, E. G. (1990). The Alternative Paradigm Dialog. In *The Paradigm Dialog*, E. Guba (Ed.), Sage Publications: London, pp 17 – 30

Guest, G., MacQueen, K., and Namey, E. E. (2012) *Applied thematic analysis*. Thousand Oaks, CA: SAGE

Guest, G. (2013). Describing Mixed Methods Research: An Alternative to Typologies. *Journal of Mixed Methods Research, 7*(2), 141-151. doi: 10.1177/1558689812461179

Gupta, Babita, Dasgupta, Subhasish, & Gupta, Atul. (2008). Adoption of ICT in a government organization in a developing country: An empirical study. *The Journal of Strategic Information Systems, 17*(2), 140-154. doi: http://dx.doi.org/10.1016/j.jsis.2007.12.004

Gurau, C. (2002). E-banking in transition economies: The case of Romania. *Journal of Financial Services Marketing,* 6(4), 362–378.

Habermas, J. (1987). The Theory of Communicative Action. *Volume Two: Lifeworld and System,* Translated by T.McCarthy. Boston, MA: Beacon.

Haddon, L. (2000) Social Exclusion and Information and Communication Technologies: Lessons from Studies of Single parents and the Young Elderly, *New Media Society*, Volume 2, p387.

Haggard, P. (2008) Human volition: towards a neuroscience of will. *Nature Reviews Neuroscience*, Volume 9. Pp 934 – 946. Doi: 10.1038/nrn2497

Halderman, J.A., and Teague, V (2015) The New South Wales ivote system: Security Failures and verification flaws in a live online election, *International Conference on E-voting and Identity*, pp: 35-53 retrieved from: https://arxiv.org/pdf/1504.05646.pdf

Hale, J. L., Householder, B. J., & Greene, K. L. (2002). The Theory of Reasoned Action. In J. Dillard & M. Pfau (Eds.), *The persuasion handbook: developments in theory and practice* (pp. 259 - 286). California: SAGE Publications.

Hammel, J. (2004) Assistive Technology as tools for everyday living and community participation while aging. In D. Burdick and S. Kwon (Eds), *Gerontechnology: Research and practice in technology and aging: A textbook and reference for multiple disciplines* (pp 119 -0 132) New York: Springer Publishing Company.

Harbison, J., Coughlan, A., Beaulieu, M., Karabanow, J., Vanderplaat, M., Wilderman, S., and Wrexler, E. (2012) Understanding "Elder Abuse and Neglect": A Critique of Assumptions Underpinning Responses to the Mistreatment and Neglect of Older People, *Journal of Elder Abuse and Neglect*, Volume 24, Issue 12. Pp 88 – 103.

Harley, D., and Abrams, R. (2009). Whatever happened to the unlikely lads? A hoaxing metamorphosis, *Virus Bulletin 2009 Conference Proceedings,* Accessed November 15th 2015 from http://www.eset.com/us/resources/white-papers/Harlet-Abrams-VB2009.pdf

Harley, D., Grooten, M., Burn, S., & Johnston, C. (2012). *My PC has 32539 Errors: How Telephone Support Scams really work*. Paper presented at the Virus Bulletin Conference (VB 2012), Fairmont Dallas Hotel, Dallas. http://go.eset.com/us/resources/white-papers/Harley-etal-VB2012.pdf

Harmo, P., Taipalus, T., Knuuttila, J., Vallet, J., and Halme, A. (2005) Needs and Solutions – Home Automation and Service Robots for the Elderly and Disabled. *International Conference on Intelligent Robots and Systems* (IROS, 2005). pp 3201 – 3206   DOI: 10.1109/IROS.2005.1545387

Harpur, P. (2014) Oh the Irony: Retailers blind to discrimination and lost business. *The Conversation*, Accessed August 14th 2016 from: http://theconversation.com/oh-the-irony-retailers-blind-to-discrimination-and-lost-business-33879

Hart, C.W., and Johnson, M.D. (1999) Growing the trust relationship. *Marketing Management*, Volume 8, Issue 1, pp 9 – 19.

Hartwick, J., & Barki, H. (1994). Explaining the Role of User Participation in Information System Use. *Management Science, 40*(4), 440-465. doi: 10.2307/2632752

Heaney, C.A., and Israel, B.A. (2002) Social networks and social support. In K.Glanz, B.K. Rimer, and F.M. Lewis (Eds) *Health behaviour and health education*. San Fransisco: Jossey-Bass.

Heather, J., Ryan, P.Y.E, & Teague, V., (2010) Pretty Good Democracy for more expressive voting systems, in Computer Security – ESORICS 2010: Volume 6345 of the series Lecture Notes in Computer Science, pp 405 – 423. http://link.springer.com/chapter/10.1007/978-3-642-15497-3_25

Henman, P. (2010) *Governing Electronically: E-Government and the Reconfiguration of Public Administration, Policy and Power*. Palgrave-Macmillan, New York.

Higgins, S.H., and Shanklin, W.L. (1992) Seeking Mass Market Acceptance for High Technology Consumer Products. *Journal of Consumer Marketing,* Volume 9 Issue 1, pp 5 – 14.

Hill, R., Beynon-Davies, P. Williams, M.D. (2008). Older people and internet engagement: Acknowledging social moderators of internet adoption, access and use, *Information, Technology and People*, Volume 21. No. 3, pp 244 – 266.

Hinde, S. (2004) Spyware: the spy in the computer. *Computer Fraud and Security*, Volume 2004 pp 15 – 16

Ho, G., Kiff, L.M., Plocher, T., and Haigh, K.Z. (2015) A Model of Trust and Reliance of Automation Technology for Older Users. *AAAI Fall Symposium on Caring Machines*, November 2005, Washington, D.C.

Hogeboom, D.L., McDermott, R.J., Perrin. K.M., Osman, H., and Bell-Ellison, B.A. (2010) Internet Use and Social Networking Among Middle Aged and Older Adults, *Educational Gerontology*, Volume 36, Issue 2.

Hollier, S. (2013) *Media Access Australia: Helping Seniors with Disabilities get online Accessibility features in popular computer and mobile devices*, Council of the Ageing

Holstein, J. A. And Gubrium, J. F. (2008). The Constructionist Mosaic. *Handbook of Constructionist Research*, Jaber F. Gubrium and James A. Holstein (Eds). Guildford Press. New York

Hopkins, D. (1985) *A Teacher's Guide to Classroom Research*. Milton Keynes: Open University Press.

Horrigan, J. (2008). Online Shopping. *Pew Internet & American Life Project*. Retrieved from Pew Research Center website:

Hossain, L., & Wigand, R.T. (2006). ICT Enabled Virtual Collaboration through Trust. *Journal of Computer-Mediated Communication, 10*(1). doi: DOI: 10.1111/j.1083-6101.2004.tb00233.x

Howcroft, B., Hamilton, R., and Hewer, P. (2002) Consumer attitude and the usage and adoption of home-based banking in the United Kingdom. *International Journal of Bank Marketing*, Volume 20, Issue 3, pp111 – 121

HSBC. (2013). Sign up for eStatements to save time, money and the environment, HSBC Personal internet Banking. Retrieved April 24, 2013, from: http://www.us.hsbc.com/1/2/home/personal-banking/pib/estatements

Hartwick, J. and Barki, H. (1994) Explaining the role of user participation in information use. *Management Science*, Volume 40, Issue 4, pp 440 – 465.

Ijsselsteijn, W., Nap, H.H., de Kort, Y., and Poels, K, (2007) Digital Game Design for Elderly Users, *Proceedings of the 2007 Conference on Future Play*, pp 17 – 22.

Interpol (2015) Cybercrime, Connecting Police for a safer World, accessed February 2015 from http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

Ivankova, N. V. (2013). Implementing Quality Criteria in designing and Conducting a Sequential QUAN - QUAL Mixed Methods Study of Student Engagement With Learning Applied Research Methods Online. *Journal of Mixed Methods Research, XX*((X)), 1 - 27. doi: 10.1177/1558689813487945

Ivanov, K. (1991) Critical Systems Thinking and Information Technology: Some reflections, doubts, and hopes through critical thinking critically considered, and through hypersystems, *Journal of Applied Systems Analysis,* Volume 18, pp 39 – 55.

Jacks, T., and Salam, A.F. (2009) Computer-Mediated Friendship Networks, *2009 Proceedings for the International Conference on Information Systems*, Paper 115 accessed 24th November 2016 from http://aisel.aisnet.org/icis2009

Jackson, N., Cochrane, B., and McMillan, R. (2013) Workforce participation of older workers as an element of New Zealand's Retirement Income Framework: A Review of Existing Knowledge

and Data. *A Report Commissioned by the Commission for Financial Literacy and Retirement Income*, Wellington, Accessed 24th April 2015 from: http://www.waikato.ac.nz/nidea

Jackson, S. L., (2009) *Research methods and Statistics: A critical Thinking Approach* (3rd Ed) Wadsworth, Cengage Learning. USA.

Jaeger, P.T., and Fleischmann, K. R. (2007) Public Libraries, Values, Trust and e-Government, *Information Technology and Libraries*, Volume 26, Issue 4.

Jaeger, P.T., and Xie, B. (2008) Developing Online Community Accessibility Guidelines for Persons with Disabilities and Older Adults, *Journal of Disability Policy Studies*, DOI: 10.1177/1044207308325997

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social Phishing. *Communications of the ACM*, 94 - 100.

Jakobsson, M., Tsow, A., Shah, A., Blevis, E., and Lim, Y. (2007). What instills trust? A qualitative study of phishing. *Proceedings of the 11th International Conference on Financial Crytography and 1st International Conference on Usable Security*, Berlin, Heidelberg, 2007 pp 356 – 361.

James, B.D., Boyle, P.A., and Bennett, D. A. (2014) Correlates of Susceptibility to Scams in Older Adults without Dementia, *Journal of Elder Abuse and Neglect,* Volume 26, Issue 2,

Jarvenpaa, N. (1999) Consumer trust in an internet store: a cross cultural validation. *Journal of Computer – Mediated Communications*, Volume 5, Issue 2, pp1 -35.

John, P.D., & Sutherland, R. (2004). Teaching and learning with ICT: new technology, new pedagogy? *Education, Communications & Information,* Volume 4, Issue 1. doi: 10.1080/1463631042000210971

Johns, C., and Burnie, S. (2013) *Becoming a reflective practitioner* (4Th ed.) Chichester, UK; Wiley-Blackwell.

Jonson, H. (2003). Constructing Crime against the Elderly in Swedish Crime Prevention Campaigns. *Journal of Scandinavian Studies in Criminology and Crime Prevention,* Volume 4, Issue 2, 180-203. doi: 10.1080/14043850310015474

Kane, E. J. (1981). Accelerating Inflation, Technological Innovation, and the Decreasing Effectiveness of Banking Regulation. *The Journal of Finance,* Volume 36, Issue 2, 355-367. doi: 10.2307/2327018

Kane, R.L., and West, J.C., (2005). *It shouldn't be this way: The failure of long-term care*. Nashville, TN. Vanderbilt University Press.

Kaner, C. (2003). A*n Introduction to Scenario Testing*. Accessed June 14th, 2017 from: http://www.kaner.com/pdfs/ScenarioIntroVer4.pdf

Karahanna, E., Straub, D.W., and Baroudi, J.J. (1999) Information technology adoption across time: a cross-sectional comparison of pre-adoption and post-adoption beliefs. *MIS Quarterly*, Volume 23, Issue 2. pp 183 – 213.

Karavidas, M., Lim, N.K., and Katsikas, S.L. (2005). The effects of computers on older adult users, *Computers in Human Behaviour*, Volume 21, Issue 5. pp 697 – 711.

Karger, H.J. and Stoesz, D. (2010) *American Social Welfare Policy*, 6th edition, Pearson, Boston.

Kassim, N., M., and Abdulla, A., K., M., A. (2006) The influence of attraction on internet banking: an extension to the trust-relationship commitment model, *International Journal of Bank Marketing,* Volume 24, Issue 6, pp.424 - 442

Katz, S. (2000) Busy bodies: Activity, aging, and the management of everyday life. *Journal of Aging Studies*, Volume 14, Issue 2, pp 135 – 152.

Keat, T.K., & Mohan, A. (2004). Integration of TAM Based Electronic Commerce Models for Trust. *Journal of American Academy of Business, Cambridge, 5*(1/2), 404-410.

Keightley, E., and Pickering, M. (2014) Technologies of Memory: Practices of remembering in analogue and digital photography, *New Media and Society*, Volume 16, no.4, pp 576 – 593.

Kelman, H.C. (1961) Processes of Opinion Change, *Public Information Quarterly*, Volume 25, pp 57 – 78.

Kelton, K., Fleischmann, K.R., and Wallace, W.A. (2008) Trust in digital information. *Journal of the American Society for Information Science and Technology.* Volume 59, Issue 3, pp 363-374.

Kemmis, S. and McTaggart, R. (1992). *The Action Research Planner (3ʳᵈ Edition),* Geelong, Victoria: Deakin University Press

Kennedy, C. (1964). Induced bias in innovation and the Theory of Distribution. *Economic Journal, 74*, 541 - 547.

Kerai, P., Wood, P., and Martin, M. (2014) A Pilot Study on the Views of Elderly Regional Australians of Personally controlled electronic health records, *International Journal of Medical Informatics*, Volume 83, Issue 3, pp 201 – 209.

Kerwer, D., (2005) Rules that Many Use. Governance, Volume 18, Issue 4. pp 611 – 632

Kibby, M.D. (2005) Email Forwardables: folklore in the age of the internet. New Media and Society, Volume 7, Issue 6, pp 770 – 790. Accessed February 12ᵗʰ, 2014, from: http://nms.sagepub.com/content/7/6/770.full.pdf

Kiel, J. (2005). The digital divide: Internet and e-mail use by the elderly. *Medical Informatics and the Internet in Medicine.* Volume 30, Issue 1 pp 9 – 23.

Kiger, P.J. (2006) Generation xboxers. *AARP Bulletin*, Volume 47, Issue 2. pp 3 – 4

Kim, B., and Han, I. (2009) The role of trust belief and its antecedents in a community-driven knowledge environment, *Journal of the Association for Information Science and Technology*, Volume 60, Issue 5, pp 1012 – 1026.

Kim, D., and Benbasat, I., (2006). The effect of trust-assuring arguments on consumer trust in internet stores: application of Toulmin's model of argumentation, *Information Systems Research.* Volume 17, Issue 3, pp 286–300.

Kim, D.J., Ferrin, D.L., and Rao, H.R. (2008). A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents. *Decision Support Systems*, Volume 44, Issue 2, pp 544 – 564.

Kim, H., Kim, G.J., Park, H.W., and Rice, R.E. (2007). Configurations of Relationships in Different Media. *Journal of Computer-Mediated Communication,* Volume 12, Issue 4, accessed March 29th 2014 from: http://jcmc.indiana.edu/vol2012/issue2014/kim.html

Kim, Y. S. (2008). Reviewing and Critiquing Computer Learning and Usage Among Older Adults. *Educational Gerontology,* Volume 34, Issue 8, 709-735. doi: 10.1080/03601270802000576

Kimberly, J. R. (1981). Managerial Innovation. In P. C. a. s. Nystrom, W.H. (Ed.), *Handbook of Organizational Design*, Volume 1, pp. 84 - 104. London: Oxford University Press.

King, H.C., Ureel L. C., Kumar, S., and Wallace, C. (2013). Lessons from Our Elders: Identifying Obstacles to Digital Literacy through Direct Engagement. *6th International Conference on Pervasive Technologies Related to Assistive Environments* (PETRA), Rhodes, Greece, 2013.

Kincheloe, J.L. (2012). Teachers as Researchers, Qualitative Inquiry as a Path to Empowerment (Classic Ed). London: Routledge Falmer.

Kinnear, P. R., & Gray, C. D. (2008). *SPSS Made Simple*. New York: Psychology Press.

Kobayashi, M., Hiyama, A., Miura, T., Asakawa, C., Hirose, M., & Ifukube, T. (2011). Elderly User Evaluation of Mobile Touchscreen Interactions. In P. Campos, N. Graham, J. Jorge, N. Nunes, P. Palanque & M. Winckler (Eds.), *Human-Computer Interaction – INTERACT 2011* Volume 6946, pp. 83-99, Springer, Berlin Heidelberg.

Kock, N. (2004) The three threats of action research: a discussion of methodological antidotes in the context of an information systems study. *Decision Support Systems,* Volume 37, Issue 2. pp 265 - 286

Kohl, H. (2005) New Victims: Breaking the Cycle of Victimization: *Hearing Before the US Senate Special Committee on Aging, 109th Congress*. (Statement of Senator Herb Kohl).

Koshy, V. (2009) Action research for improving educational practice. London: SAGE

Krantz-Kent, R. (2005) Variations in time use at stages of the life cycle. *Monthly Labor Review*. Volume 28, pp 38 – 45.

Krebsbach, K. (2002). Banks fight for Mexico toehold. *Bank Technology News.* Retrieved 8th March, 2015 from: http://www.vision.com/company/media/coverage/02/sep30.html

Krippendorf, K., (2004). *Content Analysis: An introduction to its methodology* (2nd Ed.) Thousand Oaks, CA: Sage.

Kritzinger, E., and Von Solms, S.H., (2010) Cyber security for home users: A new way of protection through awareness enforcement, *Computers and Security*, Volume 29, pp 840 – 847

Kuhl, J. (1985). Volitional mediators of cognitive-behavior-consistency: Self-regulatory processes and action versus state orientation. In J. Kuhl & J. Beckmann (Eds.), *Action control: From cognition to behaviour,* pp. 101-128. Berlin: Springer.

Kuhl, J., & Fuhrmann, A. (1998). Decomposing self-regulation and self-control: The volitional components inventory. In J. Heckhausen & C. S. Dweck (Eds.), *Motivation and self-regulation across the life span,* pp. 15-49. Cambridge: Cambridge University Press.

Kumar, R. (2011) Research Methodology: A step-by-step guide for beginners. Sage, Los Angeles.

Kuriyan, R., Kitner, K, & Watkins, J. (2010). ICTs, development and trust: an overview. *Information Technology & People,* Volume 23 Issue 3, pp 216 - 221. doi: 10.1108/09593841011069130 #sthash.VsZ62tVD.dpuf

Kurrle, S., and Naughtin, G. (2008). An Overview of Elder Abuse and Neglect in Australia, *Journal of Elder Abuse and Neglect,* Volume 20, Issue 2.

Kvasny, L. (2006) Social Reproduction and its Applicability for Community Informatics, The Journal of Community Informatics, Volume 2, no.2. Accessed 12th March from http://www.ci-journal.net/index.php/ciej/article/viewArticle/342/248

Kwan, W. H. (1991) Marketing of ATM Technology to the Elderly Market: An Exploratory Study Australian Marketing Educators Conference, Australia.

Kyriazopoulos, P., Samanta, I., Christou, R., and Ntanos, A. (2010) Elderly People with Disabilities in the Internet Age, in Technology Enhanced Learning for people with disabilities: Approaches and Applications P. Ordonez de Pablos, J.Zhao, and R.Tennyson (Eds) Premier Reference Source.

Lachs, M. S. and Pillemer, K., (2004) How would you like to be treated when you are 75, *The Lancet,* Volume 364, Issue 9441, p1192

Laforet, S., and Li, X., (2005) Consumers' attitudes towards online and mobile banking in China. *The International Journal of Bank Marketing,* Volume 23, Issues 4/5, pp 362 – 380.

Lam, J. C., Lee, M. K., (2006). Digital inclusiveness- Longitudinal study of Internet adoption by older adults. *Journal of Management Information Systems* Volume 22, Issue 4, pp 177-206. http://dx.doi.org/10.2753/mis0742-1222220407

Lam, J., & Lee, M. (2005). Bridging the Digital Divide - The Roles of Internet Self-Efficacy towards Learning Computer and the Internet among Elderly in Hong Kong, China. Paper presented at the System Sciences, 2005. HICSS '05. *Proceedings of the 38th Annual Hawaii International Conference on System Sciences.* Retrieved on the 4th of April 2016 from: http://dl.acm.org/citation.cfm?id=1042440&picked=prox

Lang, F. R., & Carstensen, L. L. (2002). Time counts: Future time perspective, goals, and social relationships. *Psychology and Aging,* Volume 17, Issue 1, 125-139. doi: 10.1037/0882-7974.17.1.125

Lassar, W.M., Manolis, C., and Lassar, S.S. (2005) The relationship between consumer innovativeness, personal characteristics, and online banking adoption, *International Journal of Bank Marketing*, Volume 23, Issue 2, pp 176 – 199.

Latham, R. and Sassen, S. (2005) Digital Formations: Constructing an object of study. In R. Latham & S. Sassen (Eds), *Digital Formation: IT and New Architecture in the Global Realm*, Princeton: Princeton University Press.

Laukkanen, T., Sinkkonen, S., Marke, K., and Laukkanen, P. (2007). "Innovation resistance among mature consumers". *The Journal of consumer marketing (0736-3761)*, Volume 24, Issue 7, p. 419.
DOI: 10.1108/07363760710834834

Laukkanen, T., Sinkkonen, S., and Laukkanen, P. (2009) Communication Strategies to overcome functional and psychological resistance to internet banking, *International Journal of Information Management*, Volume 29, Issue 2, pp 111 – 118.

Laukkanen, T and Kiviniemi, V. (2010). The role of information in mobile banking resistance. International Journal of Bank Marketing Volume 28, Issue 5, pp 372 – 388.

Lawhon, T, (1996) Technology Impacts Older Americans, Activities, Adaption and Aging, Volume 20, Issue 2. pp 51 – 64.

Lawhon, T., Ennis, D., & Lawhon, D. C. (1996). Senior adults and computers in the 1990s. *Educational Gerontology,* Volume 22, Issue 2, pp 193 - 201.

Leen, E.A.E., and Lang, F. R. (2013) Motivation of Computer based learning across adulthood, *Computers in Human Behaviour*, Volume 29, Issue 3, pp 975 – 983,

Lee, E., Kwon, K., and Schumann, D.W. (2005) Segmenting the non-adopter category in the diffusion of internet banking, *International Journal of Bank Marketing*, Volume 23, Issue 5, pp 414-437.

Lee, M. (2009) Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. Electronic Commerce Research and Applications, Volume 8, Issue 3. pp 130 – 141

Lee, Y. S. (2007). *Older adults' user experiences with mobile phones: identification of user clusters and user requirements.* (PhD), Faculty of the Virginia Polytechnic Institute and State University.

Leech, N., & Onwuegbuzie, A. (2009). A typology of mixed methods research designs. *Quality & Quantity,* Volume 43, 265 - 275.

Lepa, J., and Tatnall, A. (2006) Using Actor-Network Theory to Understanding Virtual Community Networks of Older People Using the Internet, *Journal of Business Systems, Governance and Ethics*, Volume 1, Issue 4.

Levasseur, M., Richard, L., Gauvin, L., & Raymond, E. (2010). Inventory and analysis of definitions of social participation found in the aging literature: Proposed taxonomy of social activities. *Social Science & Medicine,* Volume 71, Issue 12, pp 2141-2149. doi: http://dx.doi.org/10.1016/j.socscimed.2010.09.041

Lewicki, R. J., McAllister, D. J., & Bies, R. J. (1998). Trust and Distrust: New Relationships and Realities. *The Academy of Management Review,* Volume 23, Issue 3, pp 438-458. doi: 10.2307/259288

Lewin, K. (1946) Action research and minority problems. *Journal of Social Issues*, Volume 2, Issue 4, pp 33 – 46,

Li, J., Li, N., and Winsborough, W.H. (2009) Automated trust negotiation using cryptographic credentials. *ACM Transactions on Information and System Security* (TISSEC), Volume 13, Issue 1.

Liao, Z., & Cheung, M. T. (2003). Challenges to Internet E-Banking. *Communications of the ACM,* Volume 46, pp 248 - 250.

Lichtenstein, S. And Williamson, K. (2006) Understanding Consumer Adoption of Internet Banking: An Interpretive study in the Australian Banking context. *Journal of Electronic Commerce Research,* Volume 7, Issue 2.

Lin, H., (2011). An empirical investigation of mobile banking adoption: The effect of innovation attributes and knowledge-based trust. *International Journal of Information Management*. Volume 31, Issue 3.

Lin, J., Chan, H.C., and Wei, K.K. (2006) Understanding competing application usage with the theory of planned behaviour. *Journal of the American Society for Information Science and Technology*, 57, pp 1338 – 1349.

Liska, A. E. (1984). A critical examination of the causal structure of the Fishbein-Azjen model. *Social Psychology Quarterly,* Volume 47, pp 61 - 74.

Littler, D., and Melanthiou, D. (2006) Consumer perceptions of risk and uncertainty and the implications for behaviour towards innovative retail services: The case of Internet Banking, in the *Journal of Retailing and Consumer Services*, Volume 13, Issue 6, pp 431 – 443.

Liu, C., Marchewka, J.T., Lu, J., and Yu, C. (2005). Beyond concern – a privacy-trust-behavioural intention model of electronic commerce. *Information and Management*, Volume 42, pp 289 – 304

Loges, W.E., & Jung, J-Y. (2001). Exploring the Digital Divide : Internet Connectedness and Age. *Communication Research,* Volume 28, pp 536 - 562. doi: 10.1177/009365001028004007

Lofgren, K. (2012). *Qualitative Analysis of Interview Data. A Step by Step Guide.* London SAGE.

Lonsdale, P., (2004) "Old problems still out there: Why do ATMs give you the card back first?", Thoughts and Issues related to Human Computer Interaction, accessed February 12th 2015, from: http://cs.bham.ac.uk/~rxb/Teaching/HCI/blog/2004/03/old-problems-still-out-there-why-do.html

Losh, S.C. (2009) Generation versus aging, and education, occupation, gender and ethnicity effects in U.S. digital divides, *2009 Atlanta Conference on Science and Innovation Policy*, IEEE, pp 1-8 DOI: 10.1109/ACSIP.2009.5367820

Luo, X., Li, H., Zhang, J., and Shim, J.P. (2010) Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. *Decision Support Systems*, Volume 29, pp 222-234.

Maab, W. (2011) The Elderly and the Internet: How Senior Citizens Deal with Online Privacy, Chapter 17 in *Privacy Online*, S. Trepte and L Reinecke (eds) Springer-Verlag Berlin Heidelberg 2011.

Macedo, A.P., Petronilho, F., and Caine, J. (2013) Nursing Information Systems: From Documentation as Evidence to Documentation as a Support to the Clinical Decision Making, in the Handbook of Research on ICTs and Management systems for Improving Efficiency in Healthcare and Social Care, M.M. Cruz-Cunha, I.M. Miranda, and P. Goncalves (Eds). IGI Global, Hershey, USA.

Maddox, G. L. (1968). "Persistence of life style among the elderly: A longitudinal study of patterns of social activity in relation to life satisfaction". In B. L. Neugarten. *Middle Age and Aging: A Reader in Social Psychology*. Chicago: University of Chicago Press. pp. 181–183.

Magnusson, L., Hanson, E., and Nolan, M. (2005). The impact of information and communications technology on family carers of older people and professionals in Sweden. *Ageing and Society*, Volume 25, Issue 5. pp 693 – 713.

Manitoba Government (2001). *Using technology positively: Older adults mean business*, accessed March 13th 2015 from: http://www.gov.mb.ca/shas/publications/docs/fpt/business.pdf

Mannan, M., and van Oorschot, P.C. (2008) Security and Usability: The Gap in Real-World online banking. *Proceedings of the 2007 workshop on New Security Paradigms,* pp 1 – 14, Accessed January 8th 2016 from: http://www.nspw.org/papers/2007/nspw2007-mannan.pdf

Manoim, B. (2011). *Evaluation of Interfaces for Senior Citizens: BigScreenLive, Eldy and Pointerware*. Senior Projects Spring 2011. Paper 242. Bard College. Retrieved from http://digitalcommons.bard.edu/senproj_s2011/242

Manthorpe, J., Samsi, K., and Rapaport, J. (2012). Responding to the financial abuse of people with dementia: a qualitative study of safeguarding experiences in England, *International Psychogeriatrics,* Issue 9. pp 1454 - 1464.

Marr, N. E. and Prendergast, G. P.   (1993) Strategies for Retailing Technologies at Maturity: A retail Banking case study, *Journal of International Consumer Marketing*. Volume 3, Issue 3. pp 99 – 126.

Martin, N. (2009) Consumer Scams and the Elderly: preserving Independence through Shifting Default Rules, *Elder Law Journal.* Volume 17. Issue 1.

Martin, P. (2015) "Abbott government considers axing the Australian census to save money". Accessed 3rd October 2016 from: https://www.theage.com.au/

Marshall, J. J. and Heslop, L. A. (1987) Technology Acceptance in Canadian Retail Banking: A Study of Consumer Motivations and Use of ATMs. *International Journal of Bank Marketing*, Volume 16, Issue 4.

Masi, C.M., Suarez-Balcazar, Y., Cassey, M.Z., Kinney, L., and Piotrowski, Z.H. (2003) Internet access and empowerment: a community-based health initiative. *Journal of General Internal Medicine*. Volume 18, Issue 7, pp 525–530

Maskaleris, S.N., (2007) Identity Theft and Frauds against Senior citizens: Who's in your wallet? *Experience*, Volume 18, pp 15 – 22.

Mason, M. (2010). Sample Size and Saturation in PhD Studies Using Qualitative Interviews. *Forum Qualitative Social Research,* Volume 11, Issue 3.

Mathew, J. and Stone, G. (2003). "An empirical evaluation of US bank customer perceptions of the impact of technology on service delivery in the banking sector". *International Journal of Retail & Distribution Management (0959-0552)*, Volume 31, Issue 4, p. 190.

Mattila, M, Karjaluoto, H, and Pento, T. (2003) Internet banking adoption among mature customers: Early majority or laggards? *The Journal of Services Marketing,* Volume 17, Issues 4/5, pp 514 – 526.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995, p710). An Integrative Model of Organizational Trust. *The Academy of Management Review,* Volume 20, Issue 3, 709-734. doi: 10.2307/258792

Mayhorn, C. B., Rogers, W.A., & Fisk, A.D. (2004). Designing Technology Based on Cognitive Aging Principles. In D. C. Burdick & S. Kwon (Eds.), *Gerontechnology: research and practice in technology and aging.* pp. 42 - 53. New York: Springer.

McCloskey, D.W. (2006). The Importance of Ease of Use, Usefulness, and Trust to Online Consumers: An Examination of the Technology Acceptance Model with Older Customers. *Journal of Organizational and end user computing* (1546-2234), Volume 18, Issue 3, p. 47.

McConnell, A.R., Rydell, R.J., Strain, L.M., and Mackie, D.M., (2008) Forming Implicit and Explicit Attitudes towards Individuals: Social Group Association Cues. *Journal of Personality and Social Psychology*, Volume 94, Issue 5. pp792 – 807

McCoy, S., Galletta, D. F., and King, W.R., (2007) Applying TAM across cultures: the need for caution, *The European Journal of Information Systems,* Volume 16, pp 81 – 90. Accessed, 23rd July 2015: http://www.palgrave-journals.com/ejis/journal/v16/n1/full/3000659a.html

McDonald, S., & Mair, C. A. (2010). Social Capital Across the Life Course: Age and Gendered Patterns of Network Resources. *Sociological Forum,* Volume 25, Issue 2, 335-359. doi: 10.2307/40783397

McHugh, K. (2003) Three faces of ageism: Society, Image and Place. *Ageing and Society*, Volume 23, pp 165 – 185.

McKay, E. (2009). ICT Exacerbates the Human Side of the Digital Divide *Encyclopedia of Information Science and Technology, Second Edition* pp. 1794-1798: IGI Global.

McKnight, D.H., and Chervany, N.L., (2001). What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology, *International Journal of Electronic Commerce*. Volume 6, Issue 2, pp 6 296–315.

McKnight, H., Choudhury, V., & Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a web site: A trust building model. *Journal of Strategic Information Systems,* 11, 297–323.

McLean, A., (2011) Ethical frontiers of ICT and older users: cultural, pragmatic and ethical issues, *Ethics and Information Technology*, Volume 13, pp 313 – 326.

McMillan, S. J., Avery, E. J., & Macias, W. (2008). From Have Nots to Watch Dogs. *Information, Communication & Society,* Volume 11, Issue 5, 675-697. doi: 10.1080/13691180802126745

McMurtrey, M.E., Downey, J.P., Zeltmann, S.M., and McGaughey, R.E. (2011). Seniors and Technology: Results from a Field Study. *Journal of Computer Information Systems*, Volume 51, pp 22- 30.

McNiff, J. (2013). Action Research: Principles and practice, New York: Routledge.

McNiff, J. And Whitehead, J. (2002). *Action Research: Principles and Practice (2nd Edition)* London: RoutledgeFalmer.

McNiff, J. And Whitehead, J. (2005). *All you need to know about action research*. London, UK: Sage. Pp 3 – 5.

McTaggart, D. (2016) Census 2016: ABS Phone Lines Jammed with call for paper forms, Pensioners left on paper hold. *Your Life Choices*. Retrieved 4th October from: https://www.yourlifechoices.com.au/news/pensioners-left-on-census-hold

Mechlova, E., & Malcik, N. (2012). *ICT in Changes of Learning Theories*. Paper presented at the *10th IEEE International Conference on Emerging eLearning Technologies and Applications,* Stara Lesna, Slovakia. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6418326

Mendoza, A., Miller, T., Pedell, S., and Sterling, L. (2013). The role of user's emotions and associated quality goals on appropriation of systems: two case studies. *Proceedings of the 24ᵗʰ Australasian Conference on Information Systems*, Retrieved on May 10ᵗʰ 2016, from http://people.eng.unimelb.edu.au/tmiller/pubs/acis13.pdf

Merdenyan, B., Cikrikcili, O., Kocyigit, O, Chin, M.Y.S., and Salman, B. (2014) An Exploratory research on factors influencing individual's adoption of internet banking in Turkey. *International Journal of Advances in Computer Science and its Applications*. IJCSIA. Volume 4, Issue 4.

Merton, R. K. (1988). The Matthew Effect in Science, II: Cumulative Advantage and the Symbolism of Intellectual Property. *Isis, 79*(4), 606-623. doi: 10.2307/234750

Mesquita, A. (2012) User Perception and Influencing Factors of Technology in Everyday Life, IGI Global, Information Science Reference, Hershey: USA.

Metlife Mature Market Institute (2009) Broken trust: Elders, family, and finances: A study on elder financial abuse prevention. Virginia: Virginia Polytechnic Institute and State University. *European Journal of Ageing.* Volume 10. pp 313-323.

Meyer, A.D., and Goes, J.B. (1988) Organisational Assimilation of Innovations: A multi-level contextual analysis, *Academy of Management Review*. Volume 31, pp 897 – 923.

Meyer, S., and Mollenkopf, H. (2003) Home technology, smart homes and the aging user. In K.W. Schaie, H. W. Wahl, H. Mollenkopf, and F. Oswalds. (Eds). *Aging independently: Living arrangements and mobility*, pp 148 – 161, New York: Springer.

Microsoft (2015) Avoid tech support phone scams. Safety and Security Center, Microsoft. Accessed March 4ᵗʰ, 2015 from: https://www.microsoft.com/security/online-privacy/avoid-phone-scams.aspx

Mikkola, K., and Halonen, R., (2011) Nonsense – ICT Perceived by the Elderly, *Proceedings of the European, Mediterranean & Middle East Conference on Information Systems*, May 30ᵗʰ – 31ˢᵗ 2011, Athens, Greece. Accessed 12ᵗʰ February 2016 from: https://www.academia.edu/8786666/_nonsense_-_ICT_perceived_by_the_elderly

Milgram, S. (1983) Obedience to authority: An experimental view. New York: Harper Collins.

Miller, L. (2008) Foucauldian Constructionism, in the *Handbook of Constructionist Research*, James A. Holstein and Jaber F. Gubrium, (Eds). Guilford Press: New York. pp 251 – 274.

Millward, P. (2003). The ''grey digital divide'': perception, exclusion and barriers of access to the Internet for older people. *First Monday* [online] Volume 8, Issue 7, accessed from: http://www.firstmonday.org/

Milne, G.R, and Boze, M. (1999) Trust and concern in consumers' perceptions of marketing information management practices, *Journal of Interactive Marketing*, Volume 13, Issue 1, pp 5 – 24.

Minkler, M., and Holstein, M. (2008). From civil rights to … civic engagement? Concerns of two older critical gerontologists about a "new social movement" and what it portends. *Journal of Aging Studies*, Volume 22, pp 196 – 204.

Mirowsky, J., & Ross, C. E. (2008). Education and Self-Rated Health: Cumulative Advantage and its Rising Importance. *Research on Aging,* Volume 30, Issue 1, 93. doi: 10.1177/0164027507309649

Mitnick, K., and Simon, W.L. (2002) *The art of deception: Controlling the human element of security.* New York: Wiley.

Mitzner, T. L., Boron, J. B., Fausset, C. B., Adams, A. E., Charness, N., Czaja, S. J., . . . Sharit, J. (2010). Older adults talk technology: Technology usage and attitudes. *Computers in Human Behavior,* Volume 26, Issue 6, 1710-1721. doi: http://dx.doi.org/10.1016/j.chb.2010.06.020

Mollenkopf, H. (2004). Aging and Technology - Social Science approaches. In D. C. Burdick & S. Kwon (Eds.), *Gerontechnology: Research and Practice in Technology and Aging*, pp. 54 - 67. New York: Springer.

Mollenkopf, H. (2004). Technology and the Good Life: Challenges for Current and Future Generations of Aging People. In D. C. Burdick & S. Kwon (Eds.), *Gerontechnology: Research and Practice in Technology and Aging*. pp. 145 - 160. New York: Springer.

Morawczynski, O., & Miscione, G. (2008, p288). Examining trust in mobile banking transactions: The case of M-PESA in Kenya. In C. Avgerou, M. Smith & P. Besselaar (Eds.), *Social Dimensions Of Information And Communication Technology Policy*. Volume 282, pp. 287-298. Springer US.

Mordini, E., Wright, D., Wadhwa, K., De Hert, P., Mantovani, E., Thestrup, J., Steendam, G. D'Amico, A., and Vater, I. (2009) Senior Citizens and the ethics of e-inclusion, *Ethics Information Technology,* Volume 11, Issue 3, pp 203 – 220.

Morgan, R.M. and Hunt, S.D. (1994) The Commitment-Trust theory of relationship marketing. *Journal of Marketing,* Volume, 58. pp 20 -38.

Morrell, R.W., Mayhorn, C.B., and Echt, K.V. (2004) Why Older Adults Use or do Not Use the Internet. In *Gerontechnology: Research and Practice in Technology and Aging* D. Burdick and S. Kwon (Eds) Springer, New York.

Morris, A. (2007) E-Literacy and the grey digital divide: a review with recommendations. *Journal of Information Literacy*, Volume 2, Issue 3, Retrieved on 23rd April 2015 from http://jil.lboro.ac.uk/ojs/index.php/JIL/article/view/RA-V1-13-2007-2

Morris, A., Goodman, J., and Brading, H. (2007). "Internet use and non-use: views of older users". *Universal access in the information society (1615-5289)*, Volume 6, Issue 1, p. 43. DOI: 10.1007/s10209-006-0057-5

Morris, A. and Venkatesh, V. (2000). Age differences in technology adoption decisions: Implications for a changing work force. *Personnel Psychology,* Volume 53, Issue 2, pp 375 - 403.

Morris, J. M. (1994). Computer Training Needs of Older Adults. *Educational Gerontology,* Volume 20, Issue 6, pp 541-555. doi: 10.1080/0360127940200601

Morse, J. (1994). Designing funded qualitative research. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research*. Thousand Oaks, California.

Moschis, G.P. (1990). *Frameworks for studying older consumers: Present status and methodological issues*. *Working Paper No. 06-090*, CMCS Strategic Marketing Report Series. Georgia State University, Atlanta.

Moschis, G.P. (1992). *Marketing to Older Consumers,* Quorum Books, Westport, CT.

Mouallem, L. (2002). Oh No, Grandma Has a Computer: How Internet Fraud Will Take the Place of Telemarketing Fraud Targeting the Elderly. *Santa Clara Law Review,* Volume 42, Issue 2.

Moutinho, L., and Smith, A., (2000) Modelling bank customer satisfaction through mediation of attitudes towards human and automated banking, *International Journal of Bank Marketing*, Volume 18, Issue 3, pp.124 – 134.

Mujtava, S., and Pandey, P.K. (2012). The E-Governance Architecture of Global ICT Program, *International Journal of Computer Science and Telecommunications*, Volume 3, Issue 5. pp 136-140.

Mukherjee, A., and Nath, P. (2003) A Model of Trust in Online Relationship Banking, *The International Journal of Bank Marketing,* Volume 21, Issue 1, pp 5 – 15.

Murray, C., Barber, R.M., Foreman, K.J., Ozgoren, A.A. et al (2015) Global, regional, and national disability-adjusted life years (DALYs) for 306 diseases and injuries and health life expectancy (HALE) for 188 countries, 1990-2013: quantifying the epidemiological transition. *The Lancet,* Volume 386, 10009.

Mussweiler, T., & Strack, F. (2001). The semantics of anchoring. *Organizational behaviour and Human Decision Processes,* Volume 86, 234 - 255.

NBN. (2012). Broadband for Seniors Program. *NBN Benefits, Department of Broadband, Communications and the Digital Economy.* Retrieved 23rd April 2013, from http://www.nbn.gov.au/nbn-benefits/government-initiatives/households/broadband-for-seniors-program/

Neogi, P.K., and Cordell, A.J. (2010). The Internet and the Need for Governance: Learning from the Past, Coping with the Future, *Journal of Internet Banking and Commerce*, Volume 15, Issue No. 2. Accessed 24th June 2016 from: http://www.arraydev.com/commerce/jibc/

Neves, B.B., and Amaro, F. (2012) Too old for technology? How the elderly of Lisbon use and perceive ICT, *The Journal of Community Informatics*, Volume 8, Issue 1, Retrieved April 24th 2015 from: http://ci-journal.net/index.php/ciej/article/view/800/904

Niehaves, B., & Plattfaut, R. (2010). *T-Government for the citizens: Digital Divide and internet technology acceptance among the elderly.* Paper presented at the *tGov Workshop "10* (tGOV10), Brunel University, West London.

Nimrod, G. (2010) Seniors'Online Communities: A Quantitative Content Analysis, *The Gerontologist,* Volume 50, Issue 3. pp 382 – 392.

Noffke, S.E. (1997) Professional, personal, and political dimensions of action research. In M.W. Apple (Ed.), *Review of Research in Education*, Volume 22, pp. 305 – 343. Washington D.C.: American Educational Research Association.

Noffke, S. E., and Zeichner, K. M. (1987). Action research and teacher thinking. Paper presented at the annual meeting of the American Educational Research Association, Washington, DC.

Noor, T.H., and Sheng, Q.Z. (2011) Trust as a Service: A Framework for Trust Management in Cloud Environments, in A. Bouguettaya, M Hauswirth, and L, Liu (Eds): *WISE 2011,* LNCS 6997. pp 314-321, Springer-Verlag. Berlin Heidelberg 2011.

Nordhaus, W. (1973). Some sceptical thoughts on the Theory of Induced Innovations. *Quarterly Journal of Economics,* Volume 87, 208 - 219.

Norris, P. (2001). *The Digital Divide: Civic Engagement, Information Poverty and the Internet Worldwide*. London: Cambridge University Press.

Nygard, L., and Starkhammar, S. (2007). The use of everyday technology by people with dementia living alone: Mapping out the difficulties. *Aging & Mental Health*, Volume 11, Issue 5. pp 144 - 155

Obi, T., Ishmatova, D., & Iwasaki, N. (2013). Promoting ICT innovations for the ageing population in Japan. *International Journal of Medical Informatics,* Volume 82, Issue 4, pp 47-62. doi: http://dx.doi.org/10.1016/j.ijmedinf.2012.05.004

OCP. (2012). *Crime Profiles against Seniors*. Perth, Western Australia: OCP Retrieved from http://www.crimeprevention.wa.gov.au/uploads/file/Safety%20Advice%20for%20Seniors%20APR%2009.pdf.

O'Donoghue, T. (2007). Planning your qualitative research project: An introduction to interpretivist research in education. New York: Routledge.

OFT. (2012). *Can you stop the person you care for from being scammed? A guide for carers and care professionals*. Office of Fair Trading, UK: Crown Retrieved July 17th 2016, from: http://www.nottinghamcity.gov.uk/CHttpHandler.ashx?id=24663&p=0.

Ogrodnik, (2007). *Seniors as Victims of Crime*. Ottowa Canada: Statistics Canada. Retrieved June 12th 2015, from: http://www.statcan.gc.ca/pub/85f0033m/85f0033m2007014-eng.pdf.

O'Leary, Z. (2010) Researching Real-World Problems: A Guide to Methods of Inquiry, Sage: Los Angeles

Oliver, R. L., & Bearden, W. O. (1985). Crossover Effects in the Theory of Reasoned Action: A Moderating Influence Attempt. *Journal of Consumer Research,* Volume 12, Issue 3, 324-340. doi: 10.2307/254377

Olson, K.E., O'Brien, M.A., Rogers, W.A., and Charness, N. (2011) Diffusion of Technology: frequency of use for younger and older adults. *Ageing International*, Volume 36, Issue 1, pp 123 – 145.

Oppenheim, A. N. (1992). *Questionnaire Design, Interviewing and Attitude Measurement.* London, UK: Pinter.

Ott, R. (2000). Building Trust Online. *Computer Fraud & Security,* Volume 2000, Issue 2, pp 10-12. doi: http://dx.doi.org/10.1016/S1361-3723(00)02017-0

Ownby, R.L. (2006) Readability of consumer-oriented geriatric depression information on the Internet. *Clinical Gerontologist*, Volume 29, Issue 4, pp 17 – 32.

Oxendine, A., Borgida, E., Sullivan, J. L., & Jackson, M. S. (2003). The importance of trust and community in developing and maintaining a community electronic network. *International Journal of Human-Computer Studies,* Volume 58, Issue 6, pp 671-696. doi: http://dx.doi.org/10.1016/S1071-5819(03)00037-5

Paetau, M. (2003) Space and Social Order: The Challenge of Computer-Mediated Social Networks, *Journal of Sociocybernetics*, Volume 4, Issue 1, pp 23 – 35.

Palinkas, L.A., Horwitz, S.M., Green, C.A., Wisdom, J.P., Duan, N., and Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administrative Policy and Mental Health*, Volume 42, Issue 5, pp 533-544.

Pan, S., Jordan-Marsh, M., (2010). Internet use intention and adoption among Chinese older adults: From the expanded technology acceptance model perspective. *Computers in Human Behavior* Volume 26, Issue 5, 1111-1119. http://dx.doi.org/10.1016/j.chb.2010.03.015

Parasuraman, A. (2000). Technology Readiness Index (Tri): A Multiple-Item Scale to Measure Readiness to Embrace New Technologies. *Journal of Service Research,* Volume 2, Issue 4, pp 307-320. doi: 10.1177/109467050024001

Parasuraman, A., & Grewal, D. (2000). The impact of technology on the quality-value-loyalty chain: A research agenda. *Journal of the Academy of Marketing Science,* Volume 28, Issue 1, pp 168 - 174. doi: 10.1177/0092070300281015

Partel, K. (2015) Towards better Implementation: Australia's My Health record. *Australian Healthcare and Hospitals Association. Institute Issues,* Brief No. 13. Retrieved December 19th 2016 from:
http://apo.org.au/files/Resource/deeble_institute_issues_brief_no_13_partel_toward_better_implementation_my_health_record.pdf

Patriche, D., & Bajenaru, A. (2010). The take-up importance of ICT enabled services in crisis time, an evaluation of E-Banking, Internet Conferencing and E-Public Services. *Bulletin of the Transilvania University of Brasov,* Volume 3, Issue 52.

Patton, M., (2002). *Qualitative research and evaluation methods* (3rd Ed.) Thousand Oaks, CA: SAGE

Pavlou, P.A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, Volume 7, Issue 3, pp 101–134.

Peacock, S.E., & Kunemund, H. (2007). Senior Citizens and Internet Technology. *European Journal of Ageing,* Volume 4, Issue 4, pp 191 - 200. doi: 10.1007/s10433-007-0067-z

Peral-Peral, B. Arenas-Gaitan, J. and Ramon-Jeronimo, M. A. (2012) Internet Banking: Segmenting Elderly by Latent Class Cluster, in Recent Advances in Automatic Control, *Information and Communications.*

Perri, 6. (2005). The Governance of Technology. In C. Lyall & J. Tait (Eds), *New Modes of Governance: Developing an Integrated Policy Approach to Science, Technology, Risk and the Environment.* Aldershot: Ashgate Publishing Limited.

Petty, R. E., and Wegener, D. T. (1999) The Elaboration Likelihood Model: Current status and controversies, In *Dual Process Theories in Social Psychology*, S. Chaiken and Y. Trope (Eds), Guildford Press, New York.

Pew, R.W. (2003) Evolution of human-computer interaction: From memex to Bluetooth and beyond. In J. A. Jacko & A. Sears (Eds.). *The human-computer interaction handbook: Fundamentals, evolving technologies, and emerging applications*. Mahwah, New Jersey: Erlbaum.

Pew Research Center, (2014) Older Adults and Technology Use, available from: http://www.pewinternet.org/2014/04/03/older-adults-and-technology-use/

Phang, C. W., Sutanto, J., Kankanhalli, A., Yan, Li, Tan, B. C. Y., & Hock-Hai, Teo. (2006). Senior Citizens' Acceptance of Information Systems: A Study in the Context of e-Government Services. *IEEE Transactions on Engineering Management,* Volume 53, Issue 4, 555-569. doi: 10.1109/TEM.2006.883710

Phang, C. W., Yan, Li, Sutanto, J., & Kankanhalli, A. (2005, 03-06 Jan. 2005). *Senior Citizens' Adoption of E-Government: In Quest of the Antecedents of Perceived Usefulness.* Paper presented at the System Sciences, 2005. HICSS '05. Proceedings of the 38th Annual Hawaii International Conference on.

Pikkarainen, T., Pikkarainen, K., Karjalouto, H., and Pahnila, S. (2004) Consumer acceptance of online banking: an extension of the technology acceptance model, *Internet Research*, Volume 14, Issue 3, pp. 224 – 235.

Plaza, I., Martin, L., Martin, S., and Medrano, C. (2011) Mobile Applications in an aging society: Status and Trends, *Journal of Systems and Software,* Volume 84, Issue 11.

Porter, C.E., and Donthu, N. (2006) Using the technology acceptance model to explain how attitudes determine Internet usage: The role of perceived access barriers and demographics. *Journal of Business Research*, Volume 59, Issue 9, pp 999 – 1007.

Portet, F., Vacher, M., Golanski, C., Roux, C., and Meillon, B. (2013) Design and evaluation of a smart home voice interface for the elderly: Acceptability and objection aspects. *Personal and Ubiquitous Computing*, Springer: Verlag (Germany), Volume 17, Issue 1, pp 127 – 144.

Prensky, M. (2001) Digital Natives, Digital Immigrants Part 1. *On the Horizon*, Volume 9, Issue 5. retrieved Dec 15th 2015 from: http://www.emeraldinsight.com/doi/abs/10.1108/10748120110424816

Price, S. (2010). *Computing for Seniors: for the over 50s*. Warwickshire, United Kingdom: In Easy Steps Limited.

Pring, R. (2000). *Philosophy of Educational Research*. London: Continuum.

Print12. (2013). Two Sides targets Australia's top finance companies. Retrieved June 5th, 2013, from: http://print21.com.au/two-sides-targets-australias-top-finance-companies/61030

Priplata, A.A., Niemi, J.B., Harry, J.D., Lipsitz, L.A., and Collins, J.J. (2003) Vibrating insoles and balance control in elderly people, *The Lancet*, Volume 362.

Purdie, N, and Boulton-Lewis, G. (2003) The Learning Needs of Older Adults, *Educational Gerontology,* Volume 29, Issue 2. pp 129 – 149.

QSR international (2013), *NVivo Data Analysis Software*. QSR International. Retrieved April 3rd from: http://www.qsrinternational.com/

Quico, C. (2008). Seniors and the uses of media and ICT; exploring social iTV and social media sites potential to improve sociability and participation. In *Proceedings of the First International Conference on Designing Interactive User Experiences for TV and Video*. October 22 – 24, 2008 Silicon Valley, California, USA.

Raab, C.D. (2006) The Governance of Global Issues: Protecting Privacy in Personal Information, M. Koenig-Archibugi, and M. Zurn (Eds) *New Modes of Governance in the Global System: Exploring Publicness, Delegation and Inclusiveness.* Palgrave MacMillan. New York.

Ramzan, Z., and Wuest, C. (2007) Phishing Attacks: Analyzing Trends in 2006, CEAS 2007: *Fourth Conference on Email and Anti-Spam, Mountain View California,* Accessed, February 6th 2014 from:
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.161.8263&rep=rep1&type=pdf

Ranganathan, C., Seo, D., and Babad, Y. (2006) Switching behaviour of mobile users; Do users' relational investments and demographics matter? *European Journal of Information Systems*, Volume 15, pp 269 – 279.

Rashidi, P. And Mihailidis, A. (2013) A survey on ambient-assisted living tools for older adults, *Biomedical and Health Informatics*, Volume 17, Issue 3. pp 579 – 589.

Ray, C., Mondada, F., and Siegwart, R. (2008) What do people expect from robots? *International Conference on Intelligent Robots and Systems*, Nice, Italy. IEEE, DOI: 10.1109/IROS.2008.4650714

Reason, P. And Bradbury, H. (2007) Handbook of Action Research, 2nd Edition. London: Sage.

Redding, T.R., Eisenman, G., & Rugulo, J. (1998). Training in Technology for Late Adopters: Learning in Retirement, Computers for Seniors. *Journal of Instruction Delivery Systems,* Volume 12, Issue 3, pp 19-24.

Reinders, M.J., Dabholkar, P.A., Frambach, R.T. (2008) Consequences of forcing consumers to use Technology-Based self-service. *Journal of Service Research,* Volume 11, pp 107 – 123.

Reisenwitz, T., Iyer, R., Kuhlmeier, D. B., & Eastman, J. K. (2007). The elderly's internet usage: an updated look. *Journal of Consumer Marketing,* Volume 24, Issue 7, pp 406 - 418. doi: 10.1108/07363760710834825

Renaud, K., & van Biljon, J. (2008). *Predicting technology acceptance and adoption by the elderly: a qualitative study*. Paper presented at the Proceedings of the 2008 annual research conference of the South African Institute of Computer Scientists and Information Technologists on IT research in developing countries: riding the wave of technology, Wilderness, South Africa.

Reneau, J. M. (2012). *An examination of the acceptance, adoption, and diffusion of smartphone devices with senior citizens.* (Doctor of Philosophy Proposal), Nova Southeastern University. Retrieved from http://www.renejm.net/files/20120203_DiffusionAndAdoption_IdeaPaper.pdf

Rengamani, H., Upadhyaya, S., Rao, H.R., and Kumaraguru, P. (2010) Protecting senior citizens from cyber security attacks in the e-health scenario: an international perspective, *Proceedings of the sixth Annual Workshop on Cyber Security and Information Intelligence Research.* CSIIRW '10 Article No. 82.

Rhodes, R.A.W. (1996). The New Governance: Governing without Government, in *Political Studies*, 1996, XLIV. pp 652 – 667.

Rice, R.E., (2002) Primary issues in Internet use: Access, civic and community involvement, and social interaction and expression. In L.Lievrouw, A and S. Livingstone (Eds), *Handbook of new media: Social shapings and consequences of ICTs.* pp 105 – 135. London: Sage.

Richardson, M., Weaver, C.K., Zorn, T.E., (2005) 'Getting on': older New Zealanders' perceptions of computing, *New Media and Society*, Volume 7, No 2. pp 219 – 245.

Richardson, V. (1994) Conducting research on practice. *Educational Researcher*, Volume 23, Issue 5, pp 5 – 9.

Roberts, C., and Mort, M. (2009) Reshaping what counts as care: Older People, work, and new technologies, *ALTER – European Journal of Disability*, Volume 3, Issue 2, pp 138 – 158.

Robey, D. (1979). User Attitudes and Management Information System Use. *Academy of Management Journal,* Volume 22, Issue 3, 527-538. doi: 10.2307/255742

Robinson Jr., R.L., Marshall, G.W., and Stamps, M.B. (2005) Sales force use of technology: antecedents to technology acceptance, *Journal of Business Research,* Volume 58, Issue 12. pp. 1623–1631.

Rogers, E. M., (1962) *Diffusion of Innovations.* New York, Ballantine Press.

Rogers, E. M., (2002) Diffusion of Preventive Innovations, *Addictive Behaviours: An International Journal,* Volume 27, Issue 6, pp 989-993.

Rogers, E.M. (2003). *Diffusion of Innovations (5th edition)* (5th Edition ed.). New York: Free Press.

Rogers, E.M. Mayhorn, C. B., & Fisk, A.D. (2004). Technology in Everyday Life for Older Adults. In D. C. Burdick & S. Kwon (Eds.), *Gerotechnology: research and practice in technology and aging*. New York: Springer.

Roseman, G.H., and Stephenson, E.F. (2005) The effect of voting technology on voter turnout: Do computers scare the elderly?. *Public Choice*, Volume 123, Issues 1-2, pp 39 – 47.

Ross, S., & Smith, R. G. (2011). Risk factors for advance fee fraud victimisation. *Trends and Issues in Crime and Criminal justice, Australian Institute of Criminology,* no. 420. Accessed June 12th 2016 From: http://aic.gov.au/publications/current%20series/tandi/401-420/tandi420.html

Rotchanakitumnuai, S., & Speece, M. (2003). Barriers to internet banking adoption: A qualitative study among corporate customers in Thailand. International Journal of Bank Marketing. Rotter, J.B. (1967) A new scale for he measurement of interpersonal trust. *Journal of Personality*, Volume 35, Issue 4, pp 651 – 655.

Rotchanakitumnuai, S. And Speece, M. (2004) Corporate custoner perspectives on business value of Thai internet banking. *Journal of Electronic Commerce Research*, Volume 5, Issue 4, pp 270 – 286.

Rozanova, J., (2010) Discourse of successful aging in *The Globe & Mail*: Insights from critical gerontology. *Journal of Aging Studies,* Volume 24, pp 213-222.

Rubin, H. J., and Rubin, I. S. (2005). Qualitative interviewing: The art of hearing data (2nd ed.). California: Sage Publications, Inc.

Russell, C., Campbell, A., & Hughes, I. (2008). Research: Ageing, social capital and the Internet: Findings from an exploratory study of Australian 'silver surfers'. *Australasian Journal on Ageing,* Volume 27, Issue 2, pp 78-82. doi: 10.1111/j.1741-6612.2008.00284.x

Ryle, G. (2000) *The Concept of Mind.* University of Chicago Press.

Saloner, G., and Shepard, A. (1995) Adoption of Technologies with Network Effects: An Empirical Examination of the Adoption of Automated Teller Machines, *The RAND Journal of Economics*, Volume 26, Issue 3, pp 479 – 501.

Salter, L. (1999) Regime for Communication and Information Techologies, in C. Cutler, V. Haufler, and T. Porter (Eds) *Private Authority and International Affairs*.State University of New York.

Sassen, S. (2003a) Globalization or denationalization? *Review of International Political Economy,* Volume 10, Issue 1, pp 1 – 22.

Sassen, S. (2003b) Digital formations: mapping a field of Inquiry, Paper presented ate the IFIP (WG 8.2 – WG 9.4) *IS Perspectives and Challenges in the Context of Globalisation*. Athens, Greece. Retrieved on March the 15th, 2015, accessed from: http://www.aueb.gr/ifip-isglob03/proceedings/Saskia%20Paper.pdf

Saunders, E. J. (2004). Maximizing Computer Use among the elderly in rural senior centers. *Educational Gerontology,* Volume 30, Issue 7, pp 573-585. doi: 10.1080/03601270490466967

Savenstedt, S., Sandman, P. O., & Zingmark, K. (2006). The duality in using information and communication technology in elder care. *Journal of Advanced Nursing,* Volume 56, Issue 1, 17-25. doi: 10.1111/j.1365-2648.2006.03975.x

Sayago, S., and Blat, J. (2009) About the relevance of accessibility barriers in the everyday interactions of older people with the web, *Proceedings of the 2009 International Cross-Disciplinary Conference on Web Accessililty* (W4A), pp 104 – 113, DOI: 10.1145/1535654.1535682

Scamwatch. (2011). New twist on computer error message/virus scams. *Scamwatch Radar.* Retrieved May 13th, 2013, from: http://www.scamwatch.gov.au/content/index.phtml/itemId/834379

Schepers, J., and Wetzels, M. (2007) A meta-analysis of the technology acceptance model: Investigating subjective norm and moderation effects. *Information and Management*, Volume 44, pp 90 – 103.

Schipp, D. (2017) Same-sex marriage survey update: 12.3 million Aussies have voted, *News.com.au* http://www.news.com.au/lifestyle/gay-marriage/samesex-marriage-survey-update-123-million-aussies-have-voted/news-story/8bcbc8713b68771db2bb0c4df3bc8f42

Schmidt, I. (2015). The adoption of e-health services: Comprehensive analysis of the adoption setting from the user's perspective, Health Policy and Technology.

Schneier, B. (2006). *Beyond Fear: Thinking sensibly about security in an uncertain world*. United States: Springer.

Schneier, B. (2008). *Schneier on Security*. Indianapolis, Indiana: Wiley Publishing.

Schultz, R. L., & Slevin, D. P. (1975). In R. L. Schultz & D. P. Slevin (Eds.), *Implementing Operations Research / Management Science*. pp. 153 - 182. New York.

Scialfa, C.T., Ho, G., and Laberge, J. (2004) Perpetual Aspects of Gerontechnology. In *Gerontechnology: Research and Practice in Technology and Aging*, D. Burdick and S. Kwon (Eds) Springer, New York.

Seidman, I. E. (1991). *Interviewing as qualitative research: A guide for researchers in education and the social sciences*. New York: Teachers College Press.

Selwyn, N. (2004). The information aged: A qualitative study of older adults' use of information and communications technology. *Journal of Aging Studies,* Volume 18, Issue 4, 369-384. doi: http://dx.doi.org/10.1016/j.jaging.2004.06.008

Selwyn, N., Gorard, S., Furlong, J, & L, Madden. (2003). Older adults' use of information and communications technology in everyday life. *Ageing & Society,* Volume 23, Issue 5, 561-582. doi: doi:10.1017/S0144686X03001302

Sensen, O. (2013). *Kant on Moral Autonomy.* (Ed) Oliver Sensen: Cambridge University Press, ISBN 9781107004863.

Setterlund, D., Tilse. C., Wilson, J., McCawley, A., and Rosenman, L. (2007) Understanding Financial elder abuse in families: The potential of routine activities theory, *Ageing and Society*, Volume 27, Issue 4, pp 599 – 614

Sheng, H., & Trimi, S. (2008). M-government: technologies, applications and challenges. *Electronic Government, an International Journal,* Volume 5, Issue 1, pp 1-18. doi: 10.1504/EG.2008.016124

Shostack, A., & Stewart, A. (2008). *The New School of Information Security*. Boston USA: Addison - Wesley, .

Silverstone, R., & Haddon, L. (1996). Design and the Domestication of Information and Communication Technologies: Technical Change and Everyday Life *Communication by Design: The Politics of Information and Communication Technologies*. pp. 44 - 74. Oxford: Oxford University.

Simon, F., and Usunier, J. (2007) Cognitive, demographic, and situational determinants of service customer preference for personnel-in-contact over self-service technology, *International Journal of Research in Marketing,* Volume 24, pp 163 – 173.

Singer, D. D., Baradwaj, B. G., & Rugemer, F. (2012). The frequency and intensity of experience in online banking use. *Journal of Internet Banking and Commerce,* Volume 17, Issue 1.

Singh, S., and Morley, C. (2009) Young Australians'privacy, security and trust in internet banking. *Proceedings of the 21st Annual Conference of the Australian Computer-Human Interaction Special Interest Group OZCHI '09*, pp 121 – 128.

Smirek, L., Henka, A., and Zimmermann, G., (2015) Giving Elderly Access in Smart Environments, In Jia Zhou and Galvriel Salvendy (Eds). *Human Aspects of IT for the Aged Population. Design for Everyday Life,* Volume 9194 of the Series: Lecture Notes in Computer Science, pp 465 – 475.

Smith, D., Menon, S., and Sivakumar, K. (2005) Online peer and editorial recommendations, trust and choice in virtual markets, *Journal of Interactive Marketing,* Volume 19, Issue 3, pp 15 – 37.

Smith, E.R., and Mackie, D.M., (2007) *Social Psychology*, p 390,

Smith, C. (2008) Technology and Web-Based Support, *American Journal of Nursing,* Volume 108, Issue 9, pp 64 – 68

Smither, J.A., and Braun, C. C. (1994) Technology and Older Adults: Factors Affecting the adoption of automatic teller machines. *Journal of General Psychology*. Volume 122, Issue 4, pp 381 – 389.

Smyth, J. (1989) Developing and sustaining critical reflection in teacher education. *Journal of Education.* Volume 40, Issue 2, pp 2-9.

Soar, J, and Su, Y. (2014) Concerns of Ageing and Interest in Assistive Technologies – Convenience Sampling of Attendees at an Aged Care Technology Exhibition in China, in K.Liu et al, (Eds): *ICISO 2014, IFIP AICT,* Volume 426, pp 412-419.

Somekh, B., and Lewin, C. (2005). *Research methods in the social sciences*. London: Sage Publications.

Stanger, T. (2015) Financial Elder Abuse costs three Billion a year, *Consumer Reports,* retrieved on November the 12th, 2016, from: http://www.consumerreports.org/cro/consumer-protection/financial-elder-abuse-costs--3-billion-----or-is-it--30-billion-

Stankovic, J. A., Insup, Lee, Mok, A., & Rajkumar, R. (2005). Opportunities and obligations for physical computing systems. *Computer,* Volume 38, Issue 11, pp 23-31. doi: 10.1109/MC.2005.386

Stark, D.P., Choplin, J.M., Mikels, J.A., and McDonnell, A.S. (2014) Complex Decision-making and cognitive aging call for enhanced protection of Seniors contemplating reverse mortgages. *Law Journal.* Volume 299.

Strauss, A.and Corbin, J. (1990) *Basics of Qualitative Research,* pp 184 – 190. London Sage Publications.

Suh, B., & Han, I. (2002). Effect of trust on customer acceptance of Internet banking. *Electronic Commerce Research and Applications,* Volume 1, pp 3–4, 247-263. doi: http://dx.doi.org/10.1016/S1567-4223(02)00017-0

Sukkar, A.A., & Hasan, H. (2005). Toward a model for the acceptance of internet banking in developing countries. *Information Technology for Development*, Volume 11, Issue 4.

Summer, A. (2007). The silver tsunami: One educational strategy for preparing to meet America's next wave of undeserved. *Journal of Health Care for the Poor and Undeserved*. Volume 18, Issue 3. pp 503 – 509.

Sun, H., and Zhang, P., (2006) The role of moderating factors in user technology acceptance, *International Journal of Human-Computer Studies.*

Suoranta, M., Mattila, M., and Munnukka, J. (2005) Technology-based services: a study on the drivers and inhibitors of mobile banking, *International Journal of Management and Decision Making*, Volume 6, Issue 1, pp 33 – 46.

Sussman, S.W., and Siegel, W. S. (2003) Informational Influence in Organisations, *An Integrated Approach to Knowledge adoption.* Volume 14, Issue 1, pp 47 – 65.

Sydney Morning Herald SMH (2013) Apple maps blamed for dangerous inaccuracies in bushfire app, in *the Sydney Morning Herald*, assessed 11th December 2015 from: http://www.smh.com.au/digital-life/digital-life-news/apple-maps-blamed-for-dangerous-inaccuracies-in-bushfire-app-20130212-2ea9w.html

Sylvester, E.L. (2004) Identity Theft: Are the Elderly targeted? *Connecticut Public Interest Law Journal.* Paper 13. http://lsr.nellco.org/uconn_cpilj/13

Tait, J. (2014) Bringing it All together: Governance and Decision-making, In *Innovation: Annual Report of the Chief Scientific Advisor: Managing Risk not avoiding it:* Evidence and Case Studies 2014, Accessed January 16th, 2016, from: http://eprints.lse.ac.uk/64539/1/14-1190b-innovation-managing-risk-evidence.pdf

Tan, B., Corbett, P.S., and Wong, Y.Y. (1999) *Information Technology Diffusion in he Asia Pacific: Perspectives on Policy, Electronic Commerce, and Education.* IGP Publishing, London UK.

Tan, M. (2011). Building Digital capital, Addressing Digital Inequality: A Perspective of Singapore's ICT Plans. Paper presented at the *PTC11 Pacific Telecommunications Council Conference.* http://www.ptc.org/ptc11/images/papers/upload/Tan_Margaret_Paper.pdf

Tanis, M., and Postmes, T. (2005) A social identity approach to trust: interpersonal perception, group membership and trusting behaviour. *European Journal of Social Psychology,* Volume 35. Issue 3. pp 413-424.

Tatnall, A., and Lepa, T.J. (2003) The Internet, e-commerce and older people: an actor-network approach to researching reasons for adoption and use, *Logistics Information Management,* Vol. 16, Issue 1, pp. 56 – 63.

Taylor, S. and Todd, P.A. (1995) Understanding information technology usage: a test of competing models. *Information Systems Research*, Volume 6. pp 144 – 176.

Taylor, R.W., Caeti, T.J., Loper, D.K., Fritsch, E.J., and Liederbach, J. (2006) *Digital Crime and Digital Terrorism.* Upper Saddle River, NJ: Pearson Prentice Hall.

Teddlie, C., & Tashakkori, A. (2009). *Foundations of mixed methods research: Integrating quantitative and qualitative approaches in the social and behavioural sciences*. Thousand Oaks: CA: Sage.

Tepe, M., and Vanhuysse, P. (2010) Elderly bias, new social risks and social spending: change and timing in eight programmes across four worlds of welfare, 1980 – 2003, *Journal of European Social Policy,* Volume 20, Issue 3, pp 217 – 234.

Thomas, T.L., (2008) Cyberskepticism: The Mind's Firewall. Foreign Military Studies Office (Army) Fort Leavenworth, Kansas. Accessed on the 23rd April, 2015, from: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA494346

Thompson, R. L., Higgins, C. A. , & Howell, J. M. (1991). Personal Computing: Toward a Conceptual Model of Utilization. *MIS Quarterly,* Volume 15, Issue 1, (March), pp 125 - 143.

Thompson, R. L., Higgins, C. A., & Howell, J. M. (1994). Influence of experience on personal computer utilization: Testing a conceptual model. *Journal of Management Information Systems,* Volume 11, Issue 1, pp 167-169.

Tinker, A., McCreadie, C., Stuchbury, R., Turner-Smith, A., Cowan, D., Bialokoz. A., Lansley, P. Bright, K., Flanagan, S, Goodacre, K and Holmans, A, (2004) *Introducing assistive technology into the exiting homes of older people: Feasibility, acceptability, costs, and outcomes,* Institute of Gerontology King's College London. King's College London and the University of Reading.

Tiong, J.K.S. (1999) Customer Acceptance of self-service technology in retail banking in Christchurch, Massey University

Tornatzsky, L. G., Eveland, J. D., Boylan, M. G., Hetzner, W.A., Johnson, E. C., Roitman, D., & Schneider, J. (1983). *The Process of Technological Innovation: Reviewing the Literature.*: National Science Foundation, Productivity Improvement research section, Division of Industrial Science and technological Innovation.

Tran, B. Q. (2004). Technologies to facilitate Health and Independent Living in Elderly Populations. In D. C. Burdick & S. Kwon (Eds.), *Gerontechnology: Research and Practice in Technology and Aging*. pp. 161 - 176. New York: Springer.

Triandis, H. C. (1980). *Values, attitudes, and interpersonal behavior*. Paper presented at the Nebraska Symposium on Motivation, Lincoln.

Turner, M., Kitchenham, B., Brereton, S., Charters, and Budgen, D. (2010) Does the technology acceptance model predict actual use? A systematic literature review. *Information and Software Technology*, Volume 52, Issue 5 pp 463 – 479.

Tzezana, R. (2017) High-probability and wild-card scenarios for future crimes and terror attacks using the internet of things, *Foresight*, Volume 19, Issue 1, pp 132 – 148.

UNDP. (2013). Human Development Report 2013, The Rise of the South: Human Progress in a Diverse World *United Nations Development Programme (UNDP)*: United Nations Development Programme (UNDP).

Ureel, L.C., and Wallace, C. (2013). Software for Senior citizens: An experiential learning course in gerontology, software usability and digital literacy,

Van Biljon, J., & Kotz, P. (2007). *Modelling the factors that influence mobile phone adoption*. Paper presented at the Proceedings of the 2007 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries, Port Elizabeth, South Africa.

Van Dijck, J. (2008) Digital Photography: Communication, Identity, Memory. *Visual Communication,* Volume 7, Issue 1, pp 57 – 76.

Van Raaij, E. M., & Schepers, J. J. L. (2008). The acceptance and use of a virtual learning environment in China. *Computers and Education, 50*(3), 838 - 852.

Vance, A, Elie-Dit-Cosaque, C., and Straub, D.W. (2008) Examining trust in information technology artifacts: the effects on system quality and culture. *Journal of Management Information Systems*, Volume 24, Issue 4, pp 73 – 100.

Vannette, D.L., Krosnick, J.A., Presser, S., Fealing, K.H. and Ruggles, S. (Eds) (2017) The Palgrave Handbook of Survey Research. London, UK: Palgrave MacMillan

Vassiliki, G., and Wilson, A., (2003) Financial Service Call Centres: Problems encountered by the grey market. *Journal of Financial Services Marketing*, Volume 7, Issue 4, pp 360 – 369.

Venkatesh, V. (2000). Determinants of Perceived Ease of Use: Integrating Control, Instrinsic Motivation, and Emotion into the Technology Acceptance Model. *Information Systems Research,* Volume 11, Issue 4, pp 342-365.

Venkatesh, V., & Bala, H. (2008). Technology Acceptance Model 3 and a Research Agenda on Interventions. *Decision Sciences,* Volume 39, Issue 2, 273-315. doi: 10.1111/j.1540-5915.2008.00192.x

Venkatesh, V., & Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science,* Volume 46, Issue 2, pp 186 - 204.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly,* Volume 27, Issue 3, 425-478. doi: 10.2307/30036540

Vergeer, M., and Pelzer, B. (2009) Consequences of media and Internet use for offline and online network capital and well-being. A causal model approach. *Journal of Computer-Mediated Communication,* Volume 15, Issue 1.

Verhagen, T., and Tan, Y.H., (2004) Perceived Risk and Trust Associated with Purchasing at Electronic Marketplaces, *Proceedings of the 12th European Conference on Information Systems (ECIS), Turku, Finland,*

Verissimo, P., Correia, M., Neves, N.F., and Sousa. P. (2008) Intrusion-Resilient Middleware Design and Validation. In *Annals of Emerging Research in Information Assurance, Security and Privacy Services,* H. R. Rao and S. Upadhyaya (eds.), Elsevier, 2008.

Vimarlund, V., and Olve, N. (2005) Economic analyses for ICT in elderly healthcare: questions and challenges. *Health Informatics Journal,* Volume 11, No. 4, pp 309-321.

Vincent, J. and Harris, L. (2009) "Early Adopter" Case Studies, in L.Budd and L. Harris (Eds), *E-Governance: Managing or Governing?* New York: Routledge,

Virokannas, H., Rahkonen, M., Luoma, I., & Sorvari, M. (2000). The 60-year-old female worker as user of new technology. *International Journal of Industrial Ergonomics,* Volume 25, Issue 5, 491-495. doi: http://dx.doi.org/10.1016/S0169-8141(99)00034-7

Wadsworth, F. (2006) The Mirror, the Magnifying Glass, the Compass and the Map: Facilitating Participatory Action Research, in Peter Reason, Hilary Bradbury (Eds.) *the Handbook of Action Research,* SAGE Publications: London.

Wagner, N., Hassanein, K., and Head, M. (2010). "Computer use by older adults: A multi-disciplinary review". *Computers in Human Behavior (0747-5632),* Volume 26, Issue 5, p. 870. DOI: 10.1016/j.chb.2010.03.029

Walczuch, R., Lemmink, J., & Streukens, S. (2007). The effect of service employees' technology readiness on technology acceptance. *Information & Management,* Volume 44, Issue 2, 206-215. doi: http://dx.doi.org/10.1016/j.im.2006.12.005

Walters, W. (2004) Some critical notes on governance, *Studies in Political Economy*, Volume 73, pp 25 - 42

Walker, R.H., Craig-Lees, M., Hecker, R., and Francis, H. (2002) Technology-enabled service delivery: An investigation of reasons affecting customer adoption and rejection, *International Journal of Service Industry Management,* Volume 13, Issue 1, pp.91 – 106.

Walker, R.M., (2006) Innovation type and diffusion: An empirical analysis of local government, *Public Administration*, Volume 84, Issue 2, pp 311 – 335.

Walsham, G. (1995) The emergence of interpretivism in IS research, *Information Systems Research*, Volume 6, Issue 4, pp 376-394.

Wang, Y. D., and Emurian, H.H. (2005) An overview of online trust: Concepts, elements, and implications. *Journal of Computers in Human Behaviour,* Volume 21, pp 105 – 125.

Warshaw, P. R. (1980). A New model for predicting behavioural intentions: An Alternative to Fishbein. *Journal of Marketing Research,* Volume 17, Issue 2, pp 153 - 172.

Waycott, J., Morgans, A., Pedell, S., Ozanne, E., Vetere, F., Kulik, L., and Davis, H. (2015) Ethics in Evaluating a Sociotechnical Intervention with socially isolated older adults, *Qualitative Health Research,* Volume 25, Issue 11, pp 1518 - 1528

Weatherall, J., & White, A. (2000). A Grounded Theory Analysis of Older Adults and Information Technology. *Educational Gerontology,* Volume 26, Issue 4, pp 371-386. doi: 10.1080/036012700407857

Wegner, D. M. (2003) *The Illusion of Conscious Will.* MIT Press, Massettchusetts.

Weijters, B., & Geuens, M. (2006). Evaluation of age-related labels by senior citizens. *Psychology and Marketing, 23*(9), 783-798. doi: 10.1002/mar.20129

Weilenmann, A. (2010). *Learning to Text: An Interaction Analytic Study of How Seniors Learn to Enter Text on Mobile Phones*. Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Atlanta, Georgia, USA.

Weiser, M. (1991). The computer for the 21st Century. Scientific American. *Scientific American, 265*(3), 94-104.

Werner, J. M., Carlson, M., Jordan-Marsh, M., and Clark, F. (2011) Predictors of Computer Use in Community-Dwelling Ethnically Diverse Older Adults. *Human Factors*, Volume 53, Issue 5, pp 431 – 447.

Westjohn, S. A., and Arnold, M. J. (2007) The Effect of Consumers' Core Self-evaluations on customer satisfaction and dissatisfaction, American Marketing Association's Summer Educator's Conference, Washington, D.C.

Westjohn, S. A., Arnold, M. J., Magnusson, P., Zdravkovic, S., & Zhou, J. (2009). Technology readiness and usage: a global-identity perspective. *Journal of the Academy of Marketing Science,* Volume 37, Issue 3, pp 250-265. doi: 10.1007/s11747-008-0130-0

Whatley, M.A., Rhodes, A., Smith, R.H., and Webster, J.M. (1999) The effect of a favor on Public and Private Compliance: How internalised is the Norm of Reciprocity?. *Basic and Applied Social Psychology*, Volume 21, Issue 3. pp 251 – 259

Whitehead, J, and McNiff, J. (2006) Action Research Living Theory. London: Sage Publications.

Whitman, M. E., & Mattord, H. J. (2010). *Management of Information Security (Third Edition)*. Boston, USA: Cengage Learning.

Wicks, A.C., Berman, S.L., and Jones, T.M. (1999) The Structure of Optimal Trust: Moral and Strategic Implications. *The Academy of Management Review*, Volume 24, Issue 1, pp 99 – 116.

Wicks, A.C and Berman, S.L. (2004). The Effects of Context on Trust in Firm-Stakeholder Relationships: The Institutional Environment, Trust Creation, and Firm Performance. *Business Ethics Quarterly*, Volume 14, Issue 1, pp 141 – 160.

Wilkens, M., (2010) Privacy and Security during life, Access after Death: Are they mutually exclusive? *Hastings Law Journal*, Volume 62. pp 1037 – 1064

Wilkowska, W., & Ziefle, M. (2009). Which Factors Form Older Adults' Acceptance of Mobile Information and Communication Technologies? In A. Holzinger & K. Miesenberger (Eds.), *HCI and Usability for e-Inclusion*. Vol. 5889, pp. 81-101: Springer Berlin Heidelberg.

Will, E.M., and Callison, C. (2006) Web presence of universities: Is higher education sending the right message online?. *Public Relations Review*, Volume 32, Issue 2, pp180 – 183.

Williams, D., Ahamed, S.I., Chu, W., Wang, M. And Chang, C. (2014) Cloud-based Synchronization for Interface Settings for Older Adults, *International Journal of Hybrid Information Technology*, Volume 7, Issue 4, pp 29 – 42.

Williams, M., Rana, N., Dwivedi, Y., & Lal, B. (2011). *Is UTAUT really used or just cited for the sake of it? A systematic review of citations of UTAUT's originating article.* Paper presented at the ECIS 2011 Proceedings.

Wilson, B., and Van Haperen, K. (2015) *Soft Systems Thinking, Methodology and the Management of Change,* London: Palgrave MacMillan.

Winter (1996). Some principles and procedures for the conduct of action research. In O. Zuber-Skerritt (ed.) *New Directions in Action Research*. London: Falmer.

Wong, D.H., Loh, C., Yap, K.B., and Bak, R. (2009) To trust or not to trust: the consumer's dilemma with E-banking. *Journal of Internet Business,* Volume 6, Issue 1.

Wong, C. Y. (2011). Exploring the Relationship Between Mobile Phone and Senior Citizens: A Malaysian Perspective. *International journal of Human-Computer Interaction (IJHCI),* Volume 2, Issue 2, p 65.

Workman, M., (2008) A test of interventions for security threats from social engineering, *Information and Computer Security*, Volume 16, Issue 5, pp 463-483.

Workman, M. (2008) Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security, *Journal of the American Society for Information Science and Technology*, Volume 59, Issue 4, pp 1 – 12.

World Health Organization, (2002) *Active ageing: A policy framework, a contribution of the World Health Organization to the Second United Nations World Assembly on ageing.* Madrid, Spain: World Health Organization.

Wright, D. (2008) *Summary of SENIOR Deliverable D1.1* Environmental scanning report prepared by, trilateral research and consulting, London, 25th May 2008

Wright, D. (2009) Good practices in e-inclusion, ethical guidance and designing a dialogue roadmap. The senior project: *Social ethical and privacy needs in ICT for older people*: A dialogue roadmap, November 2009.

WSAB, (2015) Safeguarding Adults Board Strategic Plan 2015 – 1018 - Draft, Worcestershire County Council, Accessed May 23rd, 2015, from: http://www.worcestershire.gov.uk/downloads/file/5637/safeguarding_adults_board_strategic_plan_2015_-_2018_-_draft

Wu, H., Ozok, A. A., Gurses, A. P., & Wei, J. (2009). User aspects of electronic and mobile government: results from a review of current research. *Electronic Government, an International Journal,* Volume 6, Issue 3, pp 233-251. doi: 10.1504/EG.2009.024942

Wu, Y., Damnee, S., Kerherve, H., Ware, C., and Rigaud, A., (2015) Bridging the digital divide in older adults: a study from an initiative to inform older adults about new technologies. *Clinical Interventions in Aging*, Volume 10, pp 193 – 201.

Wynekoop, J. L., Senn, J. A., & Conger, S. A. (1992). The implementation of CASE tools: An innovation diffusion approach. In K. E. K. e. a. (Eds) (Ed.), *The impact of computer supported technologies on information systems development*. pp. 25 - 41. Amsterdam: Elsevier.

Xie, B., (2003). Older Adults, Computers and the Internet: Future Directions. *Computers and the Internet:* Volume 4, Issue 2.

Xie, B. (2007) Information technology education for older adults as a continuing peer learning process: A Chinese case study. *Educational Gerontology*, Volume 33, pp 429 – 450.

Xin, L., Valacich, J. S., & Hess, T. J. (2004, 5-8 Jan. 2004). *Predicting user trust in information systems: a comparison of competing trust models.* Paper presented at the System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on.

Xiong, L., and Matthews, C. (2005). Seniors and Electronic Banking, 10th AIBF Banking and Finance Conference, Melbourne Australia.

Xu, Z, and Yuan, Y. (2009) The impact of context and incentives on mobile service adoption, *International Journal of Mobile Communications*. Volume 7, Issue 3, pp 363 DOI: 10.1504/IJMC.2009.023677

Yakov, B., Shankar, V., Sultan, F., and Urban, G.L. (2005) Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study, *Journal of Marketing*, Volume 69, pp 133- 152.

Yao, M.Z. (2011) Self Protection of Online Privacy: A Behavioural Approach, *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*, (Eds) S. Trepte and L. Reinecke, SpringerLink

Yang, J., Whitefield, M., & Boehme, K. (2007). New issues and challenges facing e-banking in rural areas: an empirical study. *International Journal of Electronic Finance,* Volume 1, Issue 3, pp 336-354.

Yap, K.B., Wong, D.H., Loh, C., and Bak, R. (2010) Offline and Online banking where to draw the line when building trust in e-banking? *International Journal of Bank Marketing*, Volume 28, Issue 1, pp 27 – 46.

Ye, C., Seo, D., Desouza, K., Papagari, S, and Jha, S (2006) Post-Adoption switching Between technology Substitutes: The Case of Web Browsers, *Proceedings of the 2006 International Conference on Information Systems* (ICIS), Association for Information Systems (AISeL) Paper 116. Accessed 25th March 2016, from: http://aisel.aisnet.org/icis2006/116

Yeow, P.H.P., Yuen, Y. Y., & Tong, D.Y.T. (2008). User acceptance of Online Banking Service in Australia. *Communications of the IBIMA, 1*.

Yi, X., and Okamoto, E., (2013) Practical Internet Voting System, *Journal of Network and Computer Applications,* Volume 36, Issue 1, pp 378 – 387.

Zeelenberg, M., Nelissen, R.M. A., Breugelmans, S.M. and Pieters, R. (2008). On emotion specificity in decision-making: Why feeling is for doing. *Judgment and Decision Making,* Volume 3, pp 18–27.

Zeithmal, V. A. and Gilly, M. C. (1987) Characteristics affecting the acceptance of Retailing Technologies: A comparison of Elderly and Non-Elderly Consumers, *Journal of Retail Banking,* Volume 63, Issue 1, pp 44-68.

Zheng, R., Spears, J, Luptak, M, and Wilby, F. (2015) Understanding Older Adults' Perceptions of Internet Use: An Exploratory Factor Analysis.

Zhou, J., Rau, P. P., & Salvendy, G. (2013). Older adults' use of smart phones: an investigation of the factors influencing the acceptance of new functions. *Behaviour & Information Technology*, 1-9. doi: 10.1080/0144929X.2013.780637

Zmud, R.W., & Apple, L.E. (1989). *Measuring Information Technology Infusion*. Unpublished Manuscript.

Zuber-Skerritt, O. (1996). Introduction. In O. Zuber-Skerritt (ed.), *New Directions in Action Research*, London: Falmer, pp 3 – 9.

Zuber-Skerritt, O., and Fletcher, M. (2007). The quality of an action research thesis in the social sciences, *Quality Assurance in Education*, Volume 15, Issue 4, pp 413 – 436.

Zuboff, S. (1988) *In the Age of the Smart Machine*. Basic Books. New York.

12 APPENDIX A: Interview Questions

This appendix details the interview questions put to respondents. They appear in the order in which they were asked to respondents.

Section 1. Qualifying Questions

Participants were asked to respond to a set of questions that helped to confirm their suitability for the study. These questions were asked to participants individually and the answers were recorded using a digital recording device. Answers were then transcribed at a later date and entered manually. Transcriptions were fed through NVivo text editors for compiling themes and commonalities.

Question 1.
Are you over the age of 65?
Question 2.
Are you retired?
Question 3.
Are you an Australian Citizen?
Question 4.
Are you on any medication that impairs you from using a computer, tablet, slate, mobile smartphone or digital device?
Question 5.
Do you think of yourself as a beginner in terms of using a computer (or a tablet, or a slate, or a smart phone)?
Question 6.
Do you think of yourself as a beginner in terms of using a computer (or tablet, or a slate, or a smartphone)?
Question 7.
Are you currently retired (or not working)? And what kind of work did you do previously?
Question 8.
Have you or your partner been interviewed for this project or any other computer research or study before?
Question 9.
Have you ever undertaken computer training of any kind, including any sessions on cyber security, identity theft, or identity training?

Section 2. Different types of ICT usage and Security practices.

Participants were asked to respond to questions that inform ICT usage in terms of communications, financial circumstances, and where security exploits might occur.

Question 1.
How often do you check your emails?
Question 2.
When you check emails, describe the process of how you do that?
Question 3.
When checking emails, what type of device or machine do you use, and what is involved in checking the email? (Prompt for Desk Top, Laptop, Slate, Tablet or Mobile Smart Phone).
Question 4.
Do you ever delete emails, or do you put them in folders? Or do you have lots of old emails that you can still access through your email account?
Question 5.
Do you use a password to access your computer?
Question 6.
Do you have more than one password, and if so, how do you remember them?
Question 7.
Does anyone else have access to your password/s, and if so why?
Question 8.
If it was easier to check emails more often, would you check them more regularly?
Question 9.
Do you still send written correspondence (ie: letters) in the postal mail? And if so how often and to what places?
Question 10.
How often do you surf the internet or look at the World Wide Web?
Question 11.
Does anybody else use your computer (or other device), and do you ever use anyone else's computer?
Question 12.
Can you tell what the difference is between a "smart phone" and an ordinary telephone? Please describe how they differ.
Question 13.
How do you check your bank balance online (ie: using a computer a different device, not at all)?
Question 14.
Do you pay bills online using a credit card or debit card?
Question 15.
Do you pay bills by using a computer to transfer money from your account to another account?
Question 16.
Do you usually withdraw money from an Automatic Teller Machine (ATM) to pay bills, or do you go into a bank?
Question 17.
Do you use an ATM machine for depositing or transferring money?
Question 18.
Do you write cheques or purchase Bank Cheques, or buy money orders from the Post Office?
Question 19.
What are the types of social media that you use or intend to use? (Prompt for Facebook, LinkedIn, and Twitter)?
Question 20.
What do you understand about the term "Cookies"?
Question 21.
What do you understand about the term "Trojans"?
Question 22.
Do you think that you have ever been deceived online? Please describe what happened.

Section 3. Describing Trust

Participants were asked to respond to questions that inform the way in which people reconcile ideas about technology trust.

Question 1.
Why do you / don't you trust computers?
Question 2.
Do you know enough about computers to feel comfortable using them for finance and banking?
Question 3.
Facebook is used by family and friends to share photos and stories. Do you use Facebook, and if so did you set it up yourself? Under what conditions would you trust someone else to set up Facebook on your computer or device for you?
Question 4.
If you have never tried an online banking application, what would be required for you to trust it without having ever used it?
Question 5.
Do you trust smartphones to store your important information? Explain your answer.

Section 4. Asking about Trust

Participants were asked to respond to questions that inform the way in which older people feel about deciding to trust or reject ICT usage.

Question 1.
How would you describe the trust that you have in using your computer to send money somewhere? If you don't have a computer, would you use someone else's computer to do this?
Question 2.
How risky is it to use your computer for online banking?
Question 3.
What would help you to feel more secure in using a computer from your home for online banking?
Question 4.
How confidential do you think your emails are from other people? (Do you think anyone else reads your emails?)
Question 5.
Has a relative or a friend or an acquaintance ever offered to help you with your online banking, and have you ever taken up the offer?
Question 6.
If you get a telephone call from the bank, under what conditions do you trust them?
Question 7.
If your bank says "before we go any further I just need to confirm some details with you" and asks you for your date of birth, address and telephone number – do you give the information over the phone?
Question 8.
An acquaintance sends you an email and asks you to join Facebook so that you can keep in touch. How do you feel about Facebook?
Question 9.
If people in your circle of friends describe an online banking application as NOT trustworthy, are you also inclined not to trust such a program?

13 APPENDIX B: Scenario Details

Section 5. Scenarios about Trust, Rejection, and Choice in the usage of ICTs

Participants were asked to respond to a range of scenarios in order to ascertain how they might act in future and hypothetical situations. The participants were asked to nominate elements that they trusted as well as those elements that they did not trust. They were also encouraged to explain when they might refuse to use technology, and when they felt that they had little or no choice about their ICT usage.

Scenario 1.
If your bank told you that it would no longer send you statements in the mail, but that you could download a statement by setting up online banking, would you trust yourself and /or a computer to keep track of your money that way? How would you feel after hearing the news that you wouldn't get postal statements anymore?

Scenario 2.
You get a phone call from a phone company saying that you have an unpaid amount of forty-two dollars and thirty-seven cents ($42.37) – and that you are about to get disconnected. The lady on the phone says that it is a courtesy call and that you can pay the bill over the phone by using a credit card. What do you do?

Scenario 3.
The government announces that it is streamlining its Pension Payment Scheme – and that from now on you must go online to receive your fortnightly payments. How do you feel about using a computer for this?

Scenario 4.
Your Medical Centre tells you that they will send out a reminder "text" message for your next appointment. Do you trust that the "sms text" message will come through, or do you write the appointment down on paper somewhere? Are you comfortable that your medical practice will send a reminder via sms? Do you trust sms messages or those who send them?

Scenario 5.
Your close friend is in hospital with a serious illness. When you go to visit your friend you notice that the nurse takes a range of measurements like temperature, blood pressure and pulse-rate, but does not write or record them on a chart at the end of the bed. Instead the nurse enters the results into a small tablet device (like an ipad) and then leaves the room. How do you feel about medical tests and results being entered onto a portable electronic device /tablet rather than written onto paper? (Note with this question each participant is shown an ipad as a tavblet indicative of the type described in the scenario).

Scenario 6.
Your travel agent informs you that your $8000 "Around the World" holiday is all confirmed, and that all you need to do is to download your e-tickets from a special account made for you. The travel agent informs you that she has emailed you the password and the login details to your email so that it will be easy for you. How do you feel about this?

Scenario 7.
You are on holiday in a foreign country and you check in to a hotel. The Hotel Clerk asks you for your Credit Card. He looks suspicious and you have a strange feeling as he takes the credit card away for a few minutes in order to make an imprint for hotel security, however you don't have a choice if you want to stay at the hotel. How do you feel about the person, the hotel, and your travel experience?

Scenario 8.
A hotel advises you that you can pay for your overseas hotel accommodation before you leave, and that you can go online to pay using a credit card. How do you feel about using your credit card to do that? Do you trust the Hotel not to use your card for other things?

Scenario 9.

Your bank advises you in a letter that if you use their new phone-banking application for paying bills, they will send you your statements for free so that you can download them on your computer, tablet or smartphone. Would this make you trust the bank more than before? Would this offer interest you? Why or Why not?

Scenario 10.

The Australian Taxation Office (ATO) announces that all tax returns must be submitted online. You are not confident to use the computer but you cannot afford to use a tax accountant. Do you trust the ATO online system for tax returns and do you trust yourself to put in a tax return using an online system?

Scenario 11.

A friend tells you that you can make free phone calls to the United Kingdom (UK) and the United States of America (USA) if you download a really great program that he has discovered. Would you try and use this system? Why or why not?

Scenario 12.

A local grocery store announces that if you use their new online program you can do all of your grocery shopping online, and it will be delivered to your door for free (as long as you order and pay online). What do you do? Would you trust a system like that? Why or why not?

14 TABLE OF FIGURES

Table of Figures

END