CONSUMER ATTITUDES TOWARDS BIOMETRIC IDENTITY AUTHENTICATION

FACTORS INFLUENCING CONSUMER ATTITUDES TOWARDS BIOMETRIC IDENTITY AUTHENTICATION TECHNOLOGY WITHIN THE CANADIAN BANKING INDUSTRY

By

Michael Breward, B. Comm., M.B.A., C.M.A.

A Thesis

Submitted to the School of Graduate Studies

in Partial Fulfillment of the Requirements

for the Degree

Doctor of Philosophy

McMaster University

DOCTOR OF PHILOSOPHY
(Business Administration)

McMaster University
Hamilton, Ontario

TITLE: Factors Influencing Consumer Attitudes Towards Biometric Identity Authentication Technology Within the Canadian Banking Industry

AUTHOR: Michael Colin Breward, B.Comm. (Queen's University)
M.B.A. (McMaster University)
C.M.A. (Ontario)

SUPERVISOR: Professor Milena Head

NUMBER OF PAGES: xi, 138

Abstract

Biometrics is the science of measuring either physiological (i.e. fingerprint, iris) or behavioural (i.e. gait, signature) characteristics for the purpose of determining or authenticating one's identity. While there has been considerable research conducted with respect to the technical aspects of biometrics, very little attention has been paid to consumer acceptability of this technology. The research presented here is a first step towards filling that void.

As such, a series of three studies were undertaken. The first study was a qualitative analysis that identified what avenues of exploration Canadian banks considered to be the most salient with respect to consumer perceptions of biometric authentication technology. This analysis consisted of semi-structured interviews with subject matter experts. The second study was also qualitative and asked consumers from across Canada what they perceived as potential benefits and concerns with biometric authentication technology being used to access their bank accounts. Based upon the results of these two studies, which were further informed by a review of technology adoption literature, a third quantitative study was carried out in which a proposed research model was tested. This model identified both contextual antecedents and innate traits that may influence consumer attitudes towards using biometrics to access their bank accounts via an automated teller machine (ATM). In addition, the aspects of control and voluntariness were manipulated, through the presentation of various scenarios, to examine their effects upon both attitude as well as the direct antecedents of privacy and security concerns and usefulness. The proposed model was assessed using structural equation modeling. In addition, ANOVAs and qualitative answers to open ended questions were examined to provide further insight as to what will enhance or impede consumer acceptance of biometric technology.

The findings suggest that the contextual factors of privacy and security concerns and usefulness have a bigger impact upon attitude as compared to innate personality traits. In addition, while voluntariness appears to have no effect, control has a significant impact upon attitude as well as privacy and security concerns and usefulness. Based upon these results, implications for theory and practice are discussed, and suggestions for future research are presented. It is hoped that this initial research spurs additional interest in examining consumer acceptability of biometrics in terms of both private and public sector applications.

Acknowledgements

This dissertation would not have been possible without the support of a number of people to whom I would like to express my gratitude.

First and foremost, none of this would have been possible without the unwavering support, guidance, and patience of my supervisor Dr. Milena Head. It was during a break in a sales meeting in downtown Toronto in April 2004 that I received her e-mail inviting me to join the program. The elation I felt upon receiving the news is still fresh in my memory. For taking a chance on a "long in the tooth" finance director and giving him a chance to fulfill a life-long dream and recast himself as a researcher, I shall be forever in your debt.

Second, I would like to thank Dr. Khaled Hassanein and Dr. Nick Bontis, my committee members. Dr. Hassanein's assistance throughout the process has been invaluable, and his e-business strategy course was instrumental in piqueing my interest in leveraging the web to attain strategic advantage. Dr. Bontis has an enthusiasm that is unsurpassed and he has further heightened my passion for higher education; professional soccer's loss is academia's, and McMaster's, gain.

Third, there are a number of professors that I have had through both graduate degrees that deserve recognition for being instrumental in getting me to this point. The feedback Dr. Norm Archer gave me in his IT strategies class sparked the thought that perhaps the dream of pursuing a Ph.D. had some basis in reality. Dr. Yufei Yuan's database management class provided me with analytical tools that had an immediate and ongoing impact throughout my career in industry, and contributed significantly towards allowing me to attain my goals in the private sector. Dr. Ali Montazemi's comments in the last couple of weeks in my last MBA class at McMaster added fuel to the fire ignited by Dr. Archer. Dr. Chris Bart's corporate governance class opened my eyes to the challenges, opportunities, and rewards that come from sitting on non-profit boards. Dr. Susan Sproule not only gave me the opportunity to assist in teaching one of her courses, she also provided very insightful and valuable feedback of my proposal. Finally, Dr. Brian Detlor's advice and encouragement throughout this whole process has been exemplary. Since Dr. Detlor and I attended the same high school at the same time, I would also like to extend an additional thanks for not circulating what I consider to be very bad, and potentially embarrassing, yearbook photos.

Fourth, the administrative support staff has truly been a pleasure to work with. The skills of Carver Lewis, Chris Skrzek and Steve Bendo saved me on many occasions. Vicki Cometto and Sandra Stephens were always there with words of support and an entertaining story such that you walked away happier than when you arrived. Finally, Carolyn Colwell has been nothing short of fantastic. She is a motivator, mother, and drill sergeant rolled into one whose door was always open and who always knew what to say.

Fifth, I would like to thank Dr. Bill Banks and Dr. John Banks at Wilfrid Laurier University for the mentorship, opportunities, and guidance they have provided.

Sixth, thank you to the faculty and staff at the College of Management and Economics at the University of Guelph, and particularly Dr. Julia Christensen Hughes, for their gracious invitation to join their amazing team.

Seventh, with respect to family, my thanks has to start with my grandmother Florence whose funeral, at the age of 103, was a celebration of a life devoted to education. That event demonstrated to me the positive and everlasting impact a teacher can have in a person's life.

Eighth, my parents David and Bianca instilled in me the value of education and continuous learning, be it formal or informal.

Ninth, there is my sister Lynda and my brothers Alan and Robert whom I get along with now but, like the vast majority of siblings, were terribly annoying throughout most of my childhood. Nonetheless, they must be thanked as they were the embodiment of the cliché "what doesn't kill you, makes you stronger"; and they made me very strong.

Tenth, my daughters Bianca and Natasha have been extremely supportive in my ongoing (they would say never ending) pursuit of formal education. While they weren't thrilled that I walked away from access to unlimited concert tickets and season tickets to the Toronto Maple Leafs and Raptors, they got over that relatively quickly and have been patient and understanding throughout this entire process.

Finally, this would never have been possible without the love, sacrifice, and financial and spiritual support of my amazing wife Katherine. She has an uncanny ability to see the possibilities in every seemingly impossible situation and makes every day that much more enjoyable by her mere presence. To her, I am eternally grateful...but she already knows that!

Table of Contents

List of Figures and Tables

Figures

Tables

Chapter 1 Introduction

1.1 Importance of Topic

The rapid growth in technology has brought considerable benefits and, unfortunately, additional threats. As more and more data are converted to, and stored in, electronic formats, the greater the necessity to ensure the security of that information from unauthorized access (Sukhai 2004). Traditionally, gaining access to sensitive information and/or secure areas has depended upon some artifact a person has, such as a card or token, or what they know, such as a password or Personal Identification Number (PIN). The explosion in technology has resulted in a proliferation of PINs and passwords across a plethora of applications that include access to one's bank accounts, home computer, work computer, web-based services, car, wireless devices, etc. (Coventry et al. 2003).

Regrettably, the onus of having to remember so many passwords often becomes unmanageable such that individuals trade security for usability and memorability (Adams and Sasse 1999). Regularly changing passwords, not using the same password across multiple applications, not using standard words, etc. are commonly cited methods of increasing security that are typically not employed by individuals due to the difficulty this creates in being able to remember them all. As such, criminals find passwords easy to guess and, once they have determined the one password a person uses, they get complete access. In addition, typical methods of access involving an artifact rely on the presumption that the person attempting to gain access is the actual owner of the said token; but this may not be the case. Individuals sometimes loan their bank card and share their PIN or password with a spouse, family member, or close friend. Some people even write their password down and keep it with the card (Coventry et al. 2003). All this despite warnings to the contrary.

A possible solution is the deployment of biometric technology. As will be described later, using biometrics for identity authentication can negate the need for both tokens and passwords as well as assuring that the person attempting to gain access is present.

The biometrics industry (which is defined as the sale of biometric technology to all organizations be they commercial, government, or law enforcement, but does not include research and development) has experienced tremendous growth in the recent past, and this is expected to continue according to the International Biometrics Group (IBG 2009a). In 2004, the biometrics market was less than $50 million, but is expected to grow to approximately $7.8 billion by 2013 IBG (2009a). This corresponds with the estimate made by ABI Research which predicts the 2013 biometrics market will be $7.3 billion up from roughly $3 billion in 2008 (Miller 2008). IBG's forecast extends to 2014 during which they foresee sales of $9.4 billion (IBG 2009a).

While the initial thrust towards the adoption of biometric tools has come from governments as they pursue the introduction of biometric enabled travel documents, such as passports, other organizations around the globe are showing considerable interest in the potential for biometrics to serve a variety of purposes as exemplified in Table 1-1. The heightened interest shown by governments has resulted in an increase in research funding. As a result, biometrics are not only becoming more reliable, they are also becoming cheaper. This development, in turn, means that those organizations strictly constrained by traditional cost-benefit analysis now see biometrics as a potential solution to increasing security.

Table 1-1: Sample of Recent Newspaper Articles Dealing with the Deployment of Biometric Technology

Author	Country	Biometric	Application
Anonymous (2009)	French	Palm-vein recognition	Graduate Management Admissions Test (GMAT)
Collins (2009)	United Kingdom	Fingerprints	School attendance records Access to school services such as cafeteria, library, etc.
Jackson (2009)	Canada	Facial recognition	Ontario Lottery and Gaming (OLG) initiative to identify and exclude addicted gamblers from casinos
Lewan (2009)	Global	Biometrics combined with Radio Frequency Identification (RFID)	Government surveillance
Miller (2009)	Global	Various	Analysis of global biometrics market - 2012
Thomas (2009)	United Kingdom	Fingerprints and facial recognition	Passports
Torregoza (2009)	Philippines	Thumbprint	2010 Elections
Wambugu (2009)	Kenya	Fingerprint	ATM access

ABI Research notes two other factors in the phenomenal growth of biometrics: interoperability and convenience. "Over the next five years, systems with multitechnology, multivendor capabilities will drive adoption in both public- and private-sector applications...ABI also notes that as biometric technology gains wider adoption, it will find use in applications where other forms of security are adequate, but where a biometric approach adds convenience" (Miller 2008, p. 11).

Given the actual and expected significant growth of the biometrics industry, it seems reasonable to suggest that the possibility of individuals coming into contact with

some form biometric identity authentication will increase considerably in the near future. The significant strides being made towards dealing with the technical issues of biometrics, particularly with respect to generating international standards that address the problem of interoperability (Bala 2008; Kleist 2007; Költzsch 2006), have resulted in this technology being deployed across a variety of applications in the both the public and private sector.

The public sector is pursuing biometrics in the interests of national security as exemplified by the use of biometrics in government-issued documentation such as passports in Britain, Singapore, and Brunei (Bala 2008). While the aspects of national security are a driving force behind governments rolling out biometrics, citizens may not be willing to participate due to the nature of the information they are being asked to provide. As such, for travelers that frequently cross the border between Canada and the United States, the Canadian and United States governments are leveraging the convenience aspect of being able to bypass customs and immigration by joining a program, known as NEXUS (Canadian Border Services Agency 2009) that uses iris scanning (Sukhai 2004).

In the private sector, companies have deployed biometrics for employee authentication thereby eliminating the possibility of one employee clocking in a colleague. Casinos use face recognition to identify problem visitors and card-counters (Sukhai 2004). "Many banks have implemented systems to improve security and protect their critical assets" (Bala 2008, p. 65). In addition, "the increasing number of phishing and identity frauds puts pressure on banks to implement transaction authorization processes that are more secure than the traditional PIN card methods" (Költzsch 2006, p. 245).

Although there has been a plethora of research on the technical aspects of biometric security technologies (Lease 2005), only limited research has been done regarding consumer acceptance of biometrics, with the Human-Computer Interaction (HCI) community having very little involvement (Coventry et al. 2003). This phenomenon may simply be a reflection of the relative immaturity of the biometrics market (Lease 2005).

This research is an attempt to help fill that void by developing and testing a research model, that draws from previous research on consumer technology acceptance, to explain why consumers are, or are not, willing to adopt biometric authentication methods. The focus of the study will be within the domain of the Canadian banking industry. The reason for choosing this industry is as follows. In cases of bank fraud (for example skimming, which is the unauthorized access to a legitimate user's account via a bogus debit card), the bank often ends up reimbursing their customer for the full amount of the loss. As a result of the pervasive issuance and use of debit and credit cards, the amount of losses that the Canadian financial industry has to absorb due to this type of fraud is substantial. As the intent behind the use of biometric authentication is to limit the

ability to perpetrate these types of frauds, it seems reasonable that banks would be interested in their customers' feelings towards using this technology to access their accounts.

Furthermore, the reason for looking specifically at the Canadian banking industry is due to its dominance by five major banks. The concentration of power within the hands of these five major banks implies that, should they want to pursue the deployment of biometrics, collectively they would appear to have the power to roll it out across the entire country. Additionally, while collectively they are powerful, they also realize that individually they do not hold enough influence with consumers to unilaterally move to a system that uses biometric identity authentication.

As organizations continue to leverage the power of technology and electronically capture greater amounts of highly personal information, there will be a growing need to ensure it is only accessible to those people with appropriate authority. Biometrics is a possible solution to this problem. However, before any widespread implementation is initiated, it would be useful to identify the concerns and benefits that presently exist in the minds of individuals. Armed with this knowledge, practitioners will then be able to develop an implementation plan that addresses the perceived concerns while leveraging the perceived benefits. It is hoped that this initial investigation will spawn additional academic research into a variety of applications of biometric authentication/identification opportunities in the both the public sector (such as the safeguarding of electronic health records) and private sector (such as employee access to customer data). From the management standpoint, it is hoped that this research identifies key attributes of those consumers willing to adopt biometric authentication thereby enabling organizations to target their campaigns to the appropriate market segment when biometrics gets rolled out in various applications.

1.2 Research Objectives

Despite the growth in the use of biometric identity authentication technology, empirical research into its acceptability on the part of the citizen/consumer is limited in terms of both the number of studies and the examination of the antecedents that may influence attitude and, ultimately, adoption. This research helps to fill that gap by proposing and validating an initial model that will also guide future research in this area as well as aid practitioners in developing appropriate strategies to leverage perceived benefits while simultaneously addressing concerns to increase the chances of success as they deploy this technology.

To achieve these objectives, three studies were conducted to answer several research questions as outlined below:

Study 1: Research Question: What avenues of exploration does the Canadian banking industry consider to be most salient with respect to consumer perceptions of biometric authentication technology?

Study 2: Research Question: What do consumers perceive as the benefits of, and what are their concerns with, the deployment of biometric authentication technology within the Canadian banking industry?

Study 3: Research Question 1: What are the factors that directly shape consumer attitudes towards biometric authentication?
Research Question 2: What are the innate individual traits that influence consumers' perceptions about biometric authentication and, ultimately, their attitude towards biometric identity authentication for financial transactions?
Research Question 3: How will consumer control of their biometric information and program voluntariness, acting alone and simultaneously, impact these factors?

The following chapters of this thesis are organized as follows. Chapter 2 is a literature review of various concepts, such as trust, privacy, security, and usefulness, that have been demonstrated to influence the attitude and willingness of individuals to adopt technology. Chapter 3 discusses preliminary qualitative research that was conducted that, in conjunction with expanding upon the concepts introduced in Chapter 2, was used to create a proposed research model for consumer acceptance of biometric authentication technology. Hypotheses to be tested in this model are developed in Chapter 3. Chapter 4 describes the research methodology, the development of the research instrument, as well as the online survey. Chapter 5 is an analysis of the results of the proposed research model; in addition, the use of an alternative simplified model is discussed. Chapter 6 discusses the results of the survey and answers to the research questions. The strengths and limitations of this research are also examined as are implications for both researchers and practitioners.

Chapter 2 Literature Review

In order to appropriately frame the proposed model, this chapter will examine some of the key issues interlinked with biometrics usage. These issues are more varied and complex than those for other technologies due to the personal nature of the data collected, and the historical and potential future usages associated with it. Also, there are a plethora of possible applications of biometric identity authentication technology that address various concerns. For example, companies may deploy biometrics as a means of eliminating the ability of co-workers signing each other in thereby establishing better control of time and attendance records and the related expenses. From the customer perspective, companies may also utilize biometrics in the interests of customer service and convenience as Singapore Airlines has done. Governments may use biometric-enabled documents to enhance their efficacy of authenticating one's identity in an effort to increase national security. Similar to for-profit organizations, governments may also employ biometrics for convenience purposes by using this technology to simplify the border crossing process for frequent travelers. In other words, there are a variety of potential applications of biometrics, each driven by different motivations. The focus of this study is the use of biometric identity authentication technology in the Canadian banking industry; and, while there are a varied number of reasons for its deployment, the key issue is that it is a means to protect both consumers and banks from financial loss. As such the review will begin by examining the crime of identity fraud (IDF).

Up until recently, IDF was considered one of the fastest growing crimes in the world (Mercuri 2006). This review will therefore turn to biometrics as a possible solution to at least some IDF. While the discussion will be brief, the thrust will be to provide an overview of various biometric measures, as well as existing applications within the business environment. Once common understanding of current biometric capabilities and applications is established, this review will then examine why biometrics cannot be analyzed using a simple technology acceptance framework. While the Technology Acceptance Model (TAM) is highly appropriate for other technologies, biometrics presents unique emotional and social implementation challenges; therefore more refined models are more appropriate. These refined models still use as their basis the Theory of Reasoned Action and Theory of Planned Behaviour that originally informed TAM.

Given the recent and significant press coverage of various security breaches involving highly personal consumer information, no model relating to biometrics would be complete without an analysis of trust. For consumers to surrender ever more personal information, especially data that can be used to commit crimes against them, trust and risk have to be relevant variables. The concept of trust is highly interlinked with consumer perceptions of privacy and security, and the emotional impact these may have on technology acceptance. Consumers are worried about the amount of private information about them being held in multiple databanks, and the seemingly lax security protocols in place to secure that information. In fact, it would seem that introducing biometrics at the

consumer level creates an interesting conundrum about control. Any organization thinking about employing biometrics as a form of authentication must convince its customers that, in order to make their information more secure, they have to give up a uniquely identifying characteristic. Control becomes key in many regards. Control of the data is only one aspect of this, and is addressed within the concepts of privacy and security. Control, however, may also refer to concepts such as whether providing data is mandatory or voluntary. This means that context of the proposed biometric application may also be highly relevant.

To conclude, this review will examine issues surrounding biometrics usage to prevent financial fraud. As such, a variety of theories and concepts that will bear on the proposed adoption model (presented in Chapter 3), will be discussed.

2.1 Identity Fraud (IDF)

Although the growth of identity fraud has slowed, it is still a significant problem (Elliott 2007; Morse 2006). While many contend that the biggest contributor to the increase in identity fraud is the explosion of the internet (Milne 2003), that is somewhat of an oversimplification. Granted, over the past few years the amount of identity fraud attributable to the internet has grown to approximately 15% (Sproule and Archer 2008); however that still means that roughly 85% of the identity fraud that is committed is done in the offline environment. Therefore, while governments and business organizations must be cognizant of the growing influence of the internet on this type of crime, they cannot lose sight of their responsibility for taking appropriate steps to limit criminals' ability to perpetrate identity fraud outside the realm of cyberspace.

2.1.1 Definition of Identity Theft (IDT) and Identity Fraud (IDF)

Practitioners and academics alike have struggled to describe the terms "identity theft" and "identity fraud". The Federal Trade Commission (FTC) broadly defines identity theft as occurring when personal information is used to commit fraud (Ramaswamy 2006). Recently, a group of Canadian researchers and subject matter experts from varying backgrounds developed the following definitions for identity theft and identity fraud. "**Identity theft (IDT)** [bold in original] [is] the unauthorized collection, possession, transfer, replication or other manipulation of another person's personal information for the purposes of committing fraud or other crimes that involve the use of a false identity. IDT includes various activities associated with the unauthorized collection of personal information (e.g. hacking, phishing, skimming, insider theft, etc.) as well as activities associated with the development of a false identity (e.g. counterfeiting, document breeding, ID trafficking, etc.). **Identity fraud (IDF)** [bold in original] is a class of crimes that may be committed with a false identity. Specifically, it is the gaining of money, goods, services, other benefits, or the avoidance of obligations, through the use of a false identity." (Sproule and Archer 2008, p. 7)

The Identity Theft Resource Center (idtheftcenter.org) suggests that there are four types of identity theft.

- "Financial identity theft. The victim's name and Social Security Number (SSN) are used to apply for telephone service, credit cards or loans, and to buy merchandise or lease cars or apartments.
- Criminal identity theft. The victim's name, address and other personal details are given to law enforcement officials during the commission of a crime. The victim is then mistakenly arrested.
- Identity cloning. The victim's private information is used by an imposter to establish a new life, complete with necessary cards, permits, and papers.
- Business-identity theft. Credit cards and bank accounts are opened in the name of a business and are then used to order merchandise or acquire loans." (Ramaswamy 2006, p. 66)

2.1.2 The Cost of IDF

In 2008, the direct losses associated with identity fraud in Canada were estimated to be approaching $2 billion for the previous twelve months (Sproule and Archer 2008); and this figure represents only the crime itself without considering the multitude of other costs associated with identity fraud. In terms of the individual, there are the very real out-of-pocket costs to repair their finances and credit rating, acquire new identification, etc. which, in 2008, amounted to $156 million (Sproule and Archer 2008). In addition, while the average time Canadian consumers require to sort out the affairs is just under 18 hours (Sproule and Archer 2008), it can extend into hundreds of hours in the more extreme cases (Petouhoff and Johnson 2006; CIFAS 2007). In some instances, the victim's finances are beyond repair such that the victim is forced to commit "pseudo-suicide" and essentially start all over again (CIFAS 2007).

The government must also dedicate scarce resources to improving safeguards in administering the creation of government identification (i.e. passports, SIN/SSN, and driver's licenses). On top of this, they also incur costs associated with capturing and prosecuting the criminals. Turning to businesses, not only do they bear the brunt of the financial losses (as they tend to refund virtually all a customer's losses if their account becomes a target for identity fraud), they also incur significant overhead monitoring for occurrences of identity fraud. The costs to businesses of preventing, detecting, investigating, and prosecuting identity fraud is estimated to be at least equal to losses due to the fraud itself (Cuganesan and Lacey 2003).

2.1.3 IDF Methods

Sproule and Archer (2008) found that only 43% of Canadian identity fraud victims know, or think they know, how their information was obtained. The Canadian figure is consistent with US data for 2005 and 2006 which report values of 47% (Javelin 2006) and 42% (Javelin 2007) respectively; although a Gartner online survey done in 2006 found that 78% of the victims knew how their information was compromised (Litan 2007). Returning to the Canadian study, of those that knew how their information was

obtained, 25% said it was due to a business transaction conducted in person, 15% said it was a business transaction conducted online, and 13% said their debit card was compromised. The remaining 10 reasons were all below 10% and included the information being stolen/accessed by someone close to them (9%), stolen purse, wallet, or documents (8%), and customer/employee records of an organization (6%) (Sproule and Archer 2008).

Only 17% of the victims knew something about the perpetrator. Of these, 60% were classified as either "stranger frauds" in that the perpetrator was a complete stranger (33%) or was an employee of an organization the victim dealt with (27%). Looking at the 40% that were classified as "friendly frauds", the three most frequently cited perpetrators were a friend or roommate (22%), a spouse or ex-spouse (9%), an acquaintance (6%)

Table 2-1 summarizes a few methods of identity fraud which, again, have direct pertinence to using biometrics as a solution in combating this crime. The degree to which biometric authentication could help mitigate all these forms of IDF (i.e. skimming credit cards) will ultimately be dependent upon how broad-based this method of authentication becomes. However, from the standpoint of access to one's bank accounts via an automated teller machine (ATM), biometrics can help thwart virtually all of these techniques since there is no need for a card or to enter a personal identification number (PIN).

Table 2-1: Methods Used to Perpetrate IDF (IBG 2009b)

Method	Definition	How biometrics can help
Skimming	Use of handheld magnetic readers to collect the victim's personal information from the magnetic strip on credit and debit cards.	No debit card required
Social Engineering	Use of misrepresentation and coercion to extract confidential information from the victim. Examples would include phishing, and telemarketing.	Confidential information becomes irrelevant
Malware	Use of viruses, worms, Trojan horses, etc., which are often included in e-mails and "free" software downloads, to monitor the victims keystrokes thereby obtaining personal information, passwords and the like.	Passwords and personal information become irrelevant
Dumpster Diving	Criminals pick through the victim's garbage in search of personal information.	Personal information becomes irrelevant
Mail Theft	Criminals pick through the victim's unlocked mailboxes in search of personal information and pre-approved credit offers. This can also be accomplished by fraudulently changing a victim's address at the post office.	
Shoulder Surfing	Criminals surreptitiously look over the shoulder of a victim as they enter their PIN, password, or other personal information. Unfortunately, the ability of cell phones to take pictures and record video has given criminals a more efficient method of gathering such private information while looking completely innocuous since they appear to be merely talking.	PINS, passwords, and other personal information become irrelevant
Account Takeover	Criminals use stolen or fake identifying documents to gain access to victims' bank, credit line, and credit card accounts and have mail redirected to a new address.	False identification is useless in getting access to someone's bank account

X-Ray Film Trap	Prior to a customer using an ATM, a criminal slips a thin piece of x-ray film into the card slot. The victim inserts their card, which is subsequently "trapped" by the film. The criminal conveniently arrives and poses as the good Samaritan. He feigns helping the customer and surreptitiously makes a mental note of the customer's PIN. When the customer leaves the ATM, the customer retrieves the card trapped in the x-ray film. Armed with the victim's legitimate card and their PIN, the criminal drains as much from the credit and/or debit card account as possible.	The card and PIN are useless in attempting to gain access to someone's bank account

2.2 Biometrics

At the heart of biometrics is the concept of identification. "In the context of information systems, the purpose of identification is very concrete: it is used to link a stream of data with a person." (Clarke, 1994, p. 7).

The word biometrics is derived from the Greek words bios (life) and metrikos (measure). Biometric measurements fall into two categories. They can be physiological, such as finger prints, or behavioural, such as voice (Zorkadis and Donos 2004). Biometrics is the science of measuring these characteristics for the purpose of determining or verifying identity (International Biometric Group 2009b; Bolle et al. 2004; Reid 2004). Just like a password, a biometric is used as a means of proving who you are; but, unlike a password, a biometric is something that is part of you as opposed to something you know and, therefore, have to remember (Hopkins 1999).

2.2.1 Definition

Biometrics-based systems can be used for both identification and authentication. Authentication answers the question "Am I who I claim to be?" In this context, the system authenticates the identity of that person and makes a yes/no decision based upon a one-to-one comparison by comparing the newly scanned data to a previously stored version (Jain et al. 2004; Hopkins 1999), as would be the case with banks using biometrics at ATMs. In other words, the individual would identify themselves and the bank's computer would retrieve the biometric information and compare it to that supplied by the individual at the ATM. Identification, on the other hand, answers the question "Who am I?" In this case, the newly acquired biometric information from an individual is compared to all available biometric data files in the database using a one-to-many comparison process (Prabhakar et al. 2003; Hopkins 1999). An example of this approach is used in law enforcement when the fingerprints found at a crime scene are compared to databases storing information of previous offenders (Reid 2004). The owner of the

fingerprint is unknown such that it must be compared to every fingerprint in the database until a match is found, presuming one exists. Although these two concepts are different, biometric systems often integrate both dimensions as identification is a repetitive execution of authentication (Zorkadis and Donos 2004).

It should also be noted that there is a difference between the biometric information that is used in law enforcement application versus what is used in commercial applications. In the former, the actual biometric itself is stored. However, in the latter, upon enrollment the biometric is converted into a mathematical expression and this is what is stored in the computer as a template for identity authentication. As such, when a person subsequently uses the system, the biometric is scanned, converted into a mathematical expression, and compared to the template on file. Based upon the established parameters of acceptability (i.e. how close the mathematical expression of the scanned biometric is to that of the template on file), access is granted or denied. Based upon the fact that, for commercial applications, a mathematical expression is stored and not the biometric has privacy and security implications as it is not possible to reverse engineer a viable three dimensional biometric from its mathematical representation.

Essentially, any physiological or behavioural characteristic can be used as a biometric identifier for authentication or identification, as long as it has the following properties (Vaclav and Zdenek 2000; Prabhakar et al. 2003).

1) **Universality**: The biometric element exists in all people.
2) **Distinctiveness**: The biometric element must be specific to each person. Even twins should not match. This has recently been an issue in the UK, in its attempt to introduce a national identity card scheme. Mike Rodd, the Director of the British Computer Society (BCS), had this to say. "Iris and fingerprint scans are not necessarily unique for each individual, with almost 100 cases of naturally duplicated identifiers existing in the UK. This duplicated personal biometric data raises another technological issue for a national UK identity card (ID) scheme. The time taken to check databases of the size being contemplated for incidences of duplicated data must be evaluated. If these checks cannot be implemented immediately, it is unlikely that the identity cards being proposed will have a long-term impact on the incidence of identity theft." (Rudall 2004, p. 1235)
3) **Permanence**: The biometric does not change with time.
4) **Collectibility**: The biometric characteristic should be quantifiable and relatively easy to collect.
5) **Performance**: For biometric-based systems to be practical, accuracy, speed, and resource requirements should be satisfied. This factor has always been a hindrance to the adoption of biometrics. However, given the asymptotic growth of technology, combined with new algorithms, this is becoming less and less of an issue (Connolly 2006; Du 2006; Heracleous and Wirtz 2006). "Innovations such as fuzzy searching technologies have already demonstrated their potential to revolutionize large scale biometric searching. In

combination, they provide scope for orders of magnitude improvements in accuracy, throughput, and price/performance over the next few years." (Hopkins 1999, p. 89)

6) **Acceptability**: This indicates the extent to which a system is accepted by the intended users and the real and perceived harmlessness in terms of both collecting the biometric measure and the application. For example, there is concern that the use of biometric-based systems will propagate, innocently and/or covertly, such that the initial intended use is expanded to include systems not agreed to by members, consumers, etc. This has become know as "function creep" (Langenderfer and Linnhoff 2005).
7) **Circumvention**: This refers to how secure the system is from attacks and attempts to penetrate it, such as using fake fingerprints.

2.2.2 Biometric Measures

Physiological traits that have been used for authentication purposes include hand vein pattern, fingernail bed, iris, retina, body odor, skin reflection, ear shape, teeth, DNA, face, hand geometry, palm, and face (Bolle et al. 2004; Jain et al. 2004). Behavioural measures that have been used include voice, gait, signature, keystroke dynamics, and lip motion (Bolle et al. 2004; Matyas and Riha 2000). Table 1-2 details pertinent information regarding various biometric measures; five of the six methods mentioned are the most popular in terms of market share (IBG 2009). Other less developed biometric applications include keystroke dynamics, signature authentication, gait recognition, scent, and earlobe measurement (Bourkhonine 2005). Based upon estimated revenues for 2009, the most widely purchased biometric authentication technologies are, from highest to lowest: fingerprints, face recognition, iris scanning, voice recognition, vein recognition, and hand geometry (IBG 2009).

Table 2-2: Types of Biometric Technologies (Boukhonine et al. 2005)

Body Part	Biometrics Type	How It Works	Advantages	Disadvantages	Usage Examples
Hands	Fingerprinting (natural physiography)	Uses unique micro and macro features of fingerprints	Easy to use, inexpensive, fingerprint databases are already available.	Less reliable than retina or iris scanning.	Access control, computer access control.
	Hand geometry (natural physiography)	Captures up to 90 unique hand characteristics	Easy to use and inexpensive.	Balky and sensitive to environment.	Access control, computer access.
Face	Face recognition (natural physiography/ appearance)	Captures characteristics of a face either from video or still image and translates them to digital form.	Suitable for identification applications, relatively unobtrusive.	Prone to errors caused by environmental influences (e.g. light), and personal changes such as facial hair, sunglasses; is expensive.	Identification (law enforcement); identity authentication.
Eyes	Iris scanning (natural physiography)	Captures unique patterns of an iris.	Secure, does not require physical contact, non-intrusive.	Expensive, sensitive to environmental conditions.	High security applications in controlled environments.
	Retina scanning (natural physiography)	Captures unique pattern of blood vessels.	Secure and accurate.	Expensive; requires perfect alignment – usually a user must look in monocular or binocular receptacle.	High security applications in controlled environments.
Voice	Voice recognition (social behaviour)	Captures unique characteristics of voice.	Easy to use and understand, non-intrusive.	Sensitive to background conditions such as noise.	Automated call centers.

2.3 Technology Acceptance Models

With technological growth accelerating and the increasing pervasiveness of computers, researchers have developed, and continue to develop, various models to explain why people adopt different types of technology. Some models have been adopted from other disciplines [such as social psychology's Theory of Reasoned Action (Ajzen and Fishbein 1980)]. Others have built upon general frameworks from other disciplines and added constructs more directly related to technology [such as the Technology

Acceptance Model, or TAM, (Davis 1989)] being derived from the Theory of Reasoned Action. Some have further adapted TAM in an attempt to adjust this model for specific contexts such as online gaming (Hsu et al. 2004), online banking (Pikkarainen et al. 2004), online shopping (Gefen et al. 2003a), and internet usage (Moon et al. 2001); and still others have examined different perspectives such as personal innovativeness (Agarwal and Prasad 1998) and computer playfulness (Webster et al. 1992).

The following two sections will briefly examine some of these models and the various constructs that have emerged as antecedents to technology adoption. The remaining sections explore the findings of previous authors with respect to the influence of innate personality traits, such as trust, risk, and innovativeness (Sections 2.3.3 through 2.3.5), as well as the impact of situation-dependant perceptions, such as privacy, security, and usefulness (Sections 2.3.6 and 2.3.7), upon consumer attitudes towards, and usage of, technology. Due to the concept of privacy receiving more research attention than that of security, privacy is examined first, with security being discussed subsequently and essentially in relation to privacy due to the inter-relationship that exists between the two concepts. This is also done to explore the intermingling of the two concepts by researchers, practitioners, and legislators which has lead to confusion in the minds of consumers such that they have difficulty discerning between the two. Usefulness is then examined from the perspective of privacy and security due to the simultaneous interaction, in the minds of consumers, of these three concepts through what Culnan and Armstrong (1999) define as a "privacy calculus". Finally, the impact of context upon technology acceptance is examined (Section 2.3.8). As previously noted, research into the acceptance of biometrics is extremely limited. Therefore, this review will look at research examining the acceptance of associated technologies such as electronic commerce, mobile commerce, and ubiquitous (i.e. anytime, anywhere) commerce. This analysis serves as the foundation upon which the proposed research model (discussed in Chapter 3) has been developed.

2.3.1 Theory of Reasoned Action (TRA) and Theory of Planned Behaviour (TPB)

The Theory of Reasoned Action (TRA), depicted in Figure 2-1, suggests that a person's actual behaviour is influenced by their behavioural intention, which is in turn influenced by their attitude toward the behaviour and subjective norm (Ajzen and Fishbein 1980; Fishbein and Ajzen 1975). Attitude toward the behaviour is defined as the positive or negative feelings a person has about performing the target behaviour (Chen et al. 2005). Subjective norm is defined as the person's perceptions about the opinions, regarding performing the target behaviour, of those people that are important to him/her (Fishbein and Ajzen 1975). While TRA has been used across a variety of disciplines including information systems research (Shih 2004; Bagozzi et al. 2001; Chang 1998; Brinberg and Durand 1983), it does not address cases where behaviour is not fully under an individual's control; this shortfall lead to the development of the Theory of Planned Behaviour (Ajzen 1991; Ajzen 1985).

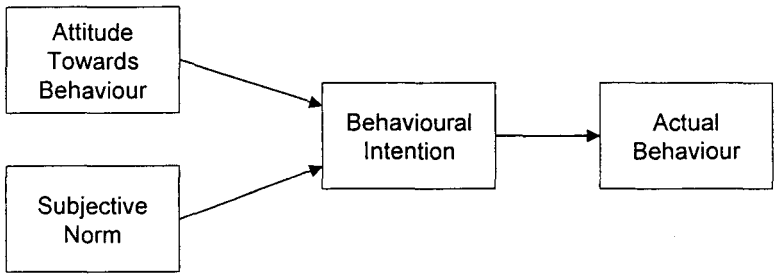


Figure 2-1: The Theory of Reasoned Action (TRA) (Ajzen and Fishbein 1980)

Like TRA, the Theory of Planned Behaviour (TPB), depicted in Figure 2-2, postulates that behavioural intention will be influenced by attitude towards the behaviour and subjective norm (Ajzen 1991; Ajzen 1985). However, in TPB a third factor is added: perceived behavioural control. Perceived behavioural control is defined as how easy or difficult it is for the individual to perform the behaviour. The addition of this factor acknowledges that while someone may be motivated to perform the behaviour, various factors may impede or enhance his/her ability to do so. Again, TPB has been utilized across various disciplines and contexts including blood donation (Giles et al. 2004), waste recycling (Chu and Chiu 2003) and information systems (Hardgrave and Johnson 2003; Taylor and Todd 1995).

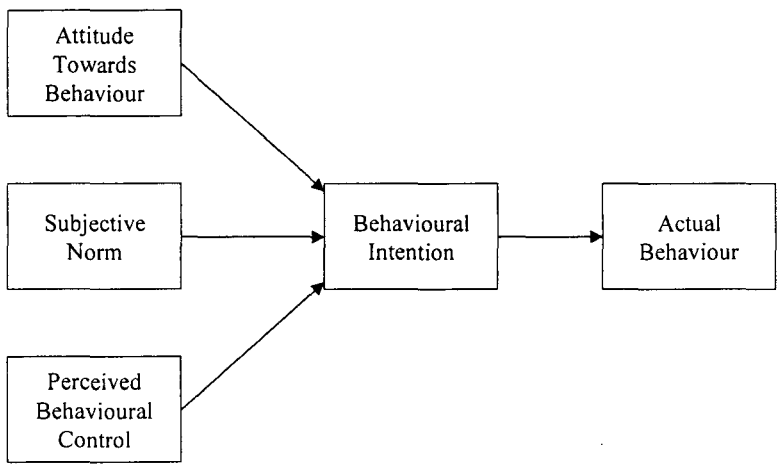


Figure 2-2: The Theory of Planned Behaviour (Ajzen 1991)

2.3.2 Technology Acceptance Model

Building upon the TRA and TPB models, the Technology Acceptance Model, depicted in Figure 2-3, was developed (Davis 1989; Davis et al 1989). While TRA and TPB are generic and therefore support cross-disciplinary application, TAM is specifically focused on examining behavioural intention to use information systems.

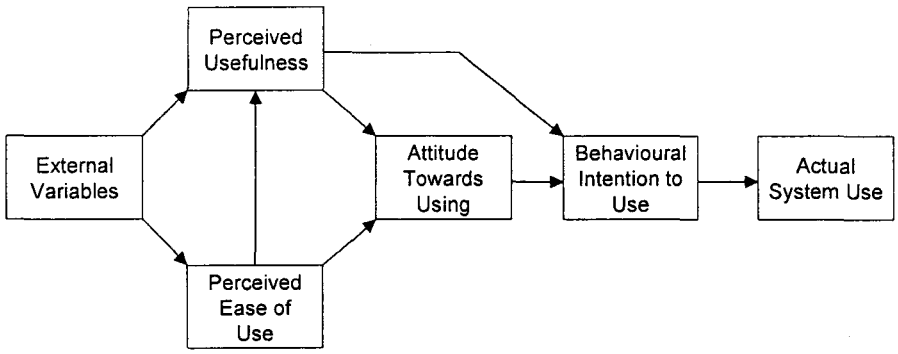


Figure 2-3: The Technology Acceptance Model (Davis et al. 1989)

Like TRA and TPB, TAM maintains that actual use is determined by behavioural intentions. However, TAM dropped social norms as an influence as it was argued that this factor is much less important in the realm of information system adoption (Davis et al. 1989). In addition, it would appear that whether or not attitude should be included as a factor influencing adoption intention is the subject of debate among researchers. Although attitude towards the behaviour was included in the original model (Davis et al. 1989) some subsequent studies dropped this factor due to its weak impact in predicting intention to adopt, or actual adoption of, an information system (Wu and Wang 2005; Venkatesh and Davis 2000), whereas other studies have demonstrated otherwise (Chen et al. 2007; Shih and Fang 2006; Venkatesh et al. 2000).

TAM postulates that the two key factors that influence usage behaviour are perceived usefulness and perceived ease of use. Perceived usefulness is defined as the degree to which an individual believes that their job performance will be enhanced by using the specified application. Perceived ease of use is defined as the degree to which an individual believes that using the specified application will be effortless (Davis et al. 1989). Furthermore, TAM suggests that perceived ease of use can influence perceived usefulness since the easier the system is to use, the more the individual is able to accomplish; conversely, the more cumbersome the system, the less work the individual is able to finish.

The original thrust of TAM was to explain behaviour within an organizational context. However, as mentioned above, with modifications it has demonstrated its applicability to a variety of other information systems adoption contexts such as electronic toll collection (Chen et al. 2007), internet banking (Shih and Fang 2006), e-commerce (Pavlou 2003), and e-services (Gefen and Straub 2003). Venkatesh et al. (2003) synthesized eight different models examining technology acceptance and developed the Unified Theory of Acceptance and Use of Technology (UTAUT) as depicted in Figure 2-4.

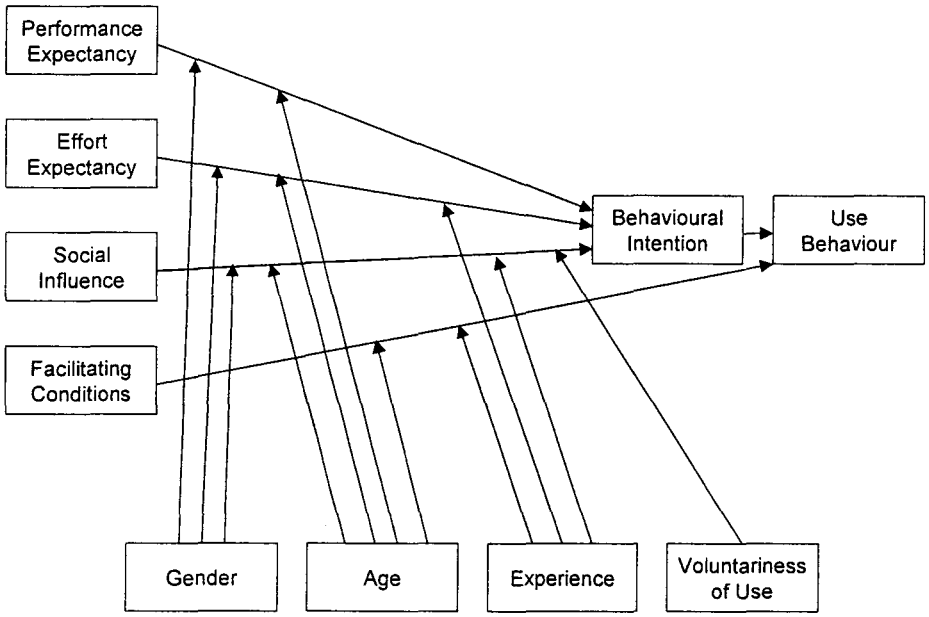


Figure 2-4: The Unified Theory of Acceptance and Use of Technology (Venkatesh et al. 2003)

2.3.3 Trust

Trust appears to be one of the more frequently investigated and yet simultaneously misunderstood concepts within social science (Das and Teng 2004). Despite the fact that the importance of trust is acknowledged in a wide variety of disciplines (such as management, political science, philosophy, sociology, marketing, and information systems) and across multiple contexts (such as romantic relationships and buyer-seller relationships), there appears to be considerable diversity with respect to its meaning, characteristics, antecedents, and outcomes (Yousafzai et al. 2003).

There is consensus that trust is a key element in examining consumer behaviour (Büttner and Göritz 2008; Chen and Barnes 2007); and, along with communication and commitment, trust is considered to be one of the cornerstones of relationship marketing theory (Flavián and Guinalíu 2006; Garbarino and Johnson 1999; Morgan and Hunt 1994). However, agreement upon a definition is allusive. This being said, the definition put forward by Mayer et al. (1995) is cited quite often in the literature. They describe trust 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 party" (Mayer et al. 1995, p.712). A subsequent meta-analysis, conducted by Rousseau et al. (1998), of trust in organizations suggested that there was fundamental agreement across various areas of research and theory in the sense that two key elements of trust were 1) vulnerability of the trustor in dealing with the trustee; and 2) the expectation that the trustee will behave in the best interests of the trustor (Yousafzai et al. 2003).

While many authors further breakdown the concept of trust into various components, an oft utilized framework looks at "...competence (ability of the trustee to do what the trustor needs), benevolence (trustee caring and motivation to act in the trustor's interests), and integrity (trustee honesty and promise keeping)" (McKnight et al. 2002, p. 337; Pavlou 2003). Furthermore, there is a wealth of dimensions of trust. Corritore et al. (2003) segmented trust along the lines of generality, kind, degree, and stage. General trust occurs in the trust one ascribes to accountants as financial professionals. Specific trust occurs when one trusts the general accountant to produce financial statements, but not to prepare taxes. Kind of trust can refer to swift trust versus slow trust as envisioned by Meyerson et al. (1996). The former occurs in the context of quickly created and dissolved relationships (such as a 3-minute online purchase from an unfamiliar vendor); whereas the latter refers to the development of trust over time and is typically seen in long term relationships, be they personal or work-related (Corritore et al. 2003). Degrees of trust run from basic (a background form of trust that is a prerequisite of social life), to guarded (trust protected by formal agreements, contracts, etc.), to extended (trust based upon openness and deep relationships where formal contracts are deemed unnecessary) (Corritore et al. 2003). Finally, trust goes through stages from initial trust development through to mature trust as the trustee demonstrates behaviour that is in keeping with the trustor's expectations (Jarvenpaa et al. 1999).

McKnight et al. (2002), looked at four high level constructs (disposition to trust, institution-based trust, trusting beliefs, and trusting intentions), and their seemingly hierarchical nature. They demonstrated that disposition to trust ["the extent to which a person displays a tendency to be willing to depend on others across a broad spectrum of situations and persons" (McKnight et al. 2002, p. 339)] positively affected institution-based trust [an individual's perceptions of the institutional environment in terms of assurances and normality (McKnight et al. 2002)] and trusting beliefs ["the confident trustor perception that the trustee has attributes that are beneficial to the trustor" (McKnight et al. 2002, p. 337)]. Trusting beliefs, in turn, were shown to positively affect trusting intentions ["the trustor is securely willing to depend, or intends to depend, on the trustee" (McKnight et al. 2002, p. 337)].

Within the realm of information systems adoption, considerable research has been done on the impact of trust, particularly with respect to e-commerce (Wang and Emurian 2005; Corritore et al. 2003; Grabner-Kraeuter and Kaluscha 2003; Grabner-Kraeuter 2002; Jarvenpaa et al. 2000). Given the nature of this trade channel (i.e. the lack of a tangible salesperson, store, etc.), this is not surprising. Various topics of research include initial trust (Chen and Barnes 2007; Hampton-Sosa and Koufaris 2005), trust in online banking (Mukherjee and Nath 2003; Yousafzai et al. 2003), trust and purchase intention (Gefen et al. 2003a), trust and online advice (McKnight et al. 2002), trust and the influence of third-party assurances (Wakefield and Whitten 2006; Kimery and McCord 2002), and trust and website type/category (Bart et al. 2005). Various studies have looked at the effect of trust in conjunction with TAM in a number of contexts such as

internet banking (Shu-Fong et al. 2007), e-commerce and older users (McCloskey 2006), mobile commerce (Wang et al. 2006), television commerce (Yu et al. 2005), and experience with online shopping (Gefen et al. 2003b).

2.3.4 Risk

The concept of risk is "one of the most pervasive in the theories of human choice" (Dowling 1986, p. 193). Risk has been investigated across a wide spectrum of disciplines such as management, public policy, finance, economics and psychology, but risk within the context of consumer behaviour seems to attract the most attention (Conchar et al. 2004). This is due to the fact that many authors believe that examining risk is necessary in order to develop an understanding of how consumers make choices (Cho and Lee 2006; Mitchell 1999; Grewal et al. 1994); some authors go so far as to suggest that risk is the core concept in understanding how consumers behave (Ingene and Hughs 1985).

Risk does not appear to have been studied extensively in terms of general information systems adoption. However, it has been studied extensively with respect to the use of the internet as a shopping channel (Büttner and Göritz 2008; Kim et al. 2008; Antony et al. 2006; Pires et al. 2004; Jarvenpaa et al. 2000). This research was fueled by practitioners and academics alike as both groups noticed that while the growth in internet purchases was substantial, it still was not as explosive as the growth in the number of consumers getting access to the internet (Cunningham et al. 2005). Findings indicated that risk has a significant negative influence on the use of the internet as a trade channel (Kim et al. 2008; Dinev et al. 2006; Cunningham et al. 2005; Forsythe and Shi 2003; Liebermann and Stahhevsky 2002). This has been attributed not only to the fact that, versus a bricks and mortar store, it is much more difficult for consumers to "experience" the product online prior to purchase (Verhagen et al. 2006), but also due to the amount of information (name, address, phone number, credit card number, etc.) a customer must submit in order to make a purchase in the first place (Kim et al. 2008; Dinev and Hart 2006). In addition, while buying products online trails internet growth, it is believed that the growth in online purchase of services, such as travel and banking, has been even slower due to the increased risk associated with the intangible nature of services relative to products (Featherman et al. 2006; Mitchell and Greatorex 1993).

In their extensive review of the literature and subsequent development of a framework on the interrelationship between trust and risk, Das and Teng (2004) observed that the notion of risk appeared in virtually every conceptualization of trust. Bhide and Stevenson (1992) went so far as to say that "aside from risk-taking...definitions and usages of trust in business have few common elements" (Bhide and Stevenson, 1992, p. 192). They point out that many scholars (e.g. Currall and Judge 1995; Sitkin and Roth 1993; Boon and Holmes 1991; Schlenker et al. 1973) argue that trust is only relevant in circumstances involving risk. Similarly, other authors (e.g. Mayer et al. 1995; Craswell 1993; Johnston-George and Swap 1982) suggest that "a sense of trust encourages risk taking by trustors" (Das and Teng 2004, p. 87).

While the concept of risk appears to overlap that of trust in the minds of individuals, a review of the literature suggests that risk would also seem to share the dubious distinction of having a similar amount of diversity, and perhaps more, in terms of meaning, constructs, models, and outcomes (Conchar et al. 2004). The net result of the exhaustive review and analysis done by Conchar et al. (2004) was "an integrated framework for the conceptualization of consumers' perceived-risk processing" (Conchar et al. 2004, p. 418). For the purposes of this study, we will be focusing upon only one aspect of Conchar et al.'s (2004) model: risk affinity.

Although Conchar et al. (2004) use the terms risk affinity and risk-taking propensity, this seems to be due to the complexity and robustness of their proposed framework. In other words, since they segmented risk down to such an extremely fine level, it appears that they did not want to get the two concepts mixed up. What they refer to as risk affinity, most authors refer to as risk propensity as is demonstrated by the following passages.

"We separate risk affinity and risk-taking propensity, treating risk affinity as an element of the consumer's individual risk profile and risk-taking propensity as a *situation specific* [italics added] outcome of risk assessment. Risk affinity is defined as a *general tendency of an individual to seek or avoid risk* [italics added], other things being equal. Simply stated, individuals who enjoy the challenge that risks entail will be more likely to undertake risky actions than those individuals who do not." (Conchar et al. 2004, p. 426)

"We regard risk propensity as a *generalized personal trait* [italics added], or an individual's general willingness to take risk...Everything else being equal...those with high risk propensity are more likely to take risks, while those with low risk propensity are less likely to do so." (Das and Teng 2004, p. 108) In keeping with the terminology employed by most authors, the term that will be used throughout the remainder of this research will be risk propensity

There has been substantial debate in the literature with regard to the term risk propensity. While some authors see it as a being stable and unchanging, others view it as being fluid yet "enduring" (Goldenson 1984, p. 757) or "persistent" (Sutherland, 1989, p. 452). These authors draw analogies to hair, which lightens when exposed to sunlight, but is basically the same colour; and to a person's face, which maintains the underlying skeletal structure, but changes with time and superficial (i.e. non reconstructive) cosmetic surgery. This "definition of risk propensity conceptualizes the construct as a cumulative tendency to take or avoid risks that is simultaneously persistent and can change over time as a result of experience" (Sitkin and Weingart 1995, p. 1575).

Reviewing the more recent literature, it would seem that the position that risk propensity is stable across situations is garnering more support, especially in more sophisticated frameworks (e.g. Conchar et al. 2004; Das and Teng 2004). It is interesting to note that the position of Das and Teng appears to have evolved over time as in previous

work they viewed risk propensity as changeable (Das and Teng 1997), more along the lines of Sitkin and Weingart (1995).

Although a more recent article (Cho and Lee 2006) suggested that risk propensity was more of a tendency than a trait, it would appear that they are referring more to the conceptualization of risk-taking propensity as espoused by Conchar et al. (2004) given that they define it within a situational context. "We identify risk propensity as another construct affecting an investor's assessment of risk with respect to the stock market" (Cho and Lee 2006, p. 114). This definition is more indicative of what most authors refer to as perceived risk in that Cho and Lee (2006) are talking about a given situation.

It has been suggested that an individual's risk propensity will ultimately affect their subjective evaluation of the situation, including perceived risk (Brockhaus 1980). "Risk-takers tend to assign more importance to gains and less importance to losses and thus underestimate the probability of losses or perceived risk. Risk-averters, on the other hand, are preoccupied with a concern for losses, so that they overestimate the probability of losses." (Das and Teng 2004, p. 108; Schneider and Lopes 1986) It has been demonstrated across a wide range of situations, such as personal investment decisions and consumer purchase decisions (Cho and Lee 2006; Conchar et al. 2004; Das and Teng 2004; Sitkin and Weingart 1995), that a consumer's risk propensity effects their risk perception. It has also been demonstrated within the context of e-commerce (López-Nicolás and Molina-Castillo 2008; Chen and He 2003).

Of particular interest is the difference in the findings of Sitkin and Weingart (1995) and Chen and He (2003) in terms of the impact upon intentions. Previous to Sitkin and Weingart's (1995) study, previous models postulated that risk propensity had a direct effect upon risk-taking behaviour. In their examination of a decision that involved a number dimensions of risk (including business, physical, and personal financial risk), Sitkin and Weingart (1995) found that risk propensity had a direct impact upon risk-taking behaviour only when risk perception was absent from the model. When perceived risk was included, there was no direct impact of risk propensity upon risk-taking behaviour; its effect was fully mediated by perceived risk. Subsequent research by Chen and He (2003), who looked at the impact of perceived risk and risk preference upon intention to adopt an online retailer, demonstrated that risk preference did have a direct impact upon adoption.

"*Risk perception* [italics in original] is defined as an individual's assessment of how risky a situation is in terms of probabilistic estimates of the degree of situational uncertainty, how controllable the situation is, and confidence in those estimates." (Sitkin and Weingart 1995, p. 1575; Baird and Thomas 1985; Bettman 1973) In terms of consumer behaviour, Bauer (1967) was one of the first to contend that purchases involve risk. Bauer "distinguishes [perceived risk] from actual risk as he argues that consumers are bounded rational actors that do not perform actual mathematical calculations of risk (unlike economic theory), and rather form subjective risk beliefs based upon internal and

external information...While consumers are notorious poor estimators of true probabilities, they are in effect reporting their perceived reality of the actual risks." (Featherman et al. 2006, p.113)

Jacoby and Kaplan (1972) identified several types of consumer perceived risk. They include financial risk, performance risk, social risk, psychological risk, physical risk, time risk, and opportunity cost. Bhatnagar et al. (2000) identified three types of risk that are most salient for consumers when shopping online. They are product, financial, and information risk. Product risk is self-explanatory, financial risk relates to the possibility of the transaction being inadvertently duplicated, and information risk is associated with privacy and security concerns (Kim et al. 2008).

Jarvenpaa et al. (2000) put forward the argument that e-vendors could increase the likelihood of consumers using them as a shopping destination if they could reduce the risk people ascribed to purchasing online. Several studies have demonstrated that the perceived risk of shopping online has negatively impacted consumer intentions to use it as a shopping channel (Kim et al. 2008; López-Nicolás and Molina-Castillo 2008; Dinev and Hart 2006; Dinev et al. 2006; Chen and He 2003; Pavlou 2003)

2.3.5 Innovativeness

Consumers that are considered innovative are broadly defined as those that seek arousal and novelty from new products (Hirunyawipada and Paswan 2006; Hirschman 1980; Midgley and Dowling 1978). They also typically demonstrate a higher level of expertise when evaluating new products and services, and tend to be early adopters relative to other members of their social or work group (Featherman et al. 2006; Rogers 1995). Like risk propensity, consumer innovativeness is usually conceptualized as a trait. "A personal trait is any characteristic by which a person differs from another in a relatively permanent and consistent way" (Hirunyawipada and Paswan 2006, p. 184; Hilgard et al. 1975). Agarwal and Prasad (1998) defined personality traits as internalized qualities of individuals that tend to remain stable across situations such that they are not influenced by specific individual or situational factors (Webster and Martocchio 1992).

Extending work done within marketing on the importance of Personal Innovativeness (PI) (Flynn and Goldsmith 1993; Midgley and Dowling 1978), Agarwal and Prasad (1998) contend that this is also an important consideration in the examination of acceptance of innovation within the realm of information technology. Based upon the marketing literature, they define Personal Innovativeness in the domain of Information Technology (PIIT) "as the willingness of an individual to try out any new information technology" (Agarwal and Prasad 1998, p. 206). They suggest that people with higher PIIT are more likely to experiment with IT innovations, demonstrate a higher degree of comfort, confidence, and expertise in their evaluation process, and are usually first to adopt them (Featherman et al. 2006).

Based upon their review of the existing theoretical and empirical research, Agarwal and Prasad (1998) contend that PIIT should be included as a key element in enhancing our understanding of innovation adoption. Other research has employed the personal innovativeness construct in various extended technology acceptance models (Cheung et al. 2005; Lassar et al. 2005; Eastlick and Lotz 1999; Agarwal and Prasad 1998). In their study of merchant adoption of a smart card-based payment system, Plouffe et al. (2001) found that "PCI [Perceived Characteristics of Innovating] belief constructs significantly outperformed TAM [Technology Acceptance Model]" (Plouffe et al. 2001, p. 219).

2.3.6 Privacy and Security

While TAM did not incorporate the constructs of privacy and security as determinants of behavioural intention to use information systems, subsequent research has included one or both of these aspects due to the nature of the technology being investigated. Throughout e-commerce adoption literature, the related aspects of privacy and security have garnered considerable attention (Chen and Barnes 2007; Van Dyke et al. 2007; Flavián and Guinalíu 2006; Sheng et al. 2006; Zhang et al. 2006; Schaupp and Bélanger 2005; Smith 2004; Joines et al. 2003; Park and Kim 2003). It has been empirically established that, despite the tremendous growth in e-commerce over the recent past (Chan and Pollard 2003; Green and Hof 2002), it would be that much greater if privacy and/or security issues were addressed more adequately in the eyes of the consumer (Swartz 2005a; Swartz 2005b; Monsuwé et al. 2004; Smith 2004; Park and Kim 2003; Saban et al. 2002; Liao and Cheung 2001; Miyazaki and Fernandez 2001; Szymanski and Hise 2000). It is estimated that, in 2000, online retail sales were reduced by $18 billion due to privacy concerns and that 92% of households with internet access do not trust online companies to keep their personal information private (FTC 2000). In another study, 52% of respondents simply abandoned an online purchase over privacy concerns (Ranganathan and Grandon 2002). One study even demonstrated that simply receiving spam resulted in a decreased use of the internet for browsing and purchasing (Saban et al. 2002). A more recent survey suggests that consumers' reticence is not abating. Sproule and Archer (2008) found concerns regarding identity fraud and theft have resulted in 20% of Canadian consumers either eliminating or reducing the amount of online shopping they do while 9% have done so with respect to online banking.

2.3.6.1 Privacy

Smith et al. (1996) developed a model that broke down an individual's privacy concerns into four dimensions: collection, unauthorized secondary use, improper access, and errors. Collection deals with the concern that organizations are collecting large amounts of data, if not too much data, which may be personally identifiable. Unauthorized secondary use is the concern that personally identifiable data will be collected for one purpose and then used for another, unintended purpose. This situation could arise when an online vendor collects information such that a customer's sign-on is easier, but then sells information about the customer's preferences, etc. to a third-party marketing firm. In one case, the online vendor found themselves in financial difficulty

and sold customer information in an attempt to shore up their finances. Improper access is more internally focused and is the concern that employees without authorized access can view personal data. This may occur when processing clerks can view both address and credit card billing data when they should have access to only one or the other. Given that insiders are sometimes found responsible for security breaches and IDF, this is a significant cause for concern. Errors refer to the possibility of inadequate internal controls such that mistakes get made or that intentional alteration can occur.

Smith et al. (1996) also tangentially mention the prospect that data may be combined. This can occur when several seemingly disparate and innocuous repositories of data are combined generating a huge reservoir of interrelated, personally identifying information that the consumer may not want to have residing on a single database, let alone disclosed (Van Dyke et al. 2007). While this example may suggest that such a situation arises somewhat arbitrarily, in other cases, there can be premeditation to slowly but surely assimilate databases such that the original, seemingly innocent application expands in ways unforeseen by the public. Langenderfer and Linnhoff (2005) refer to this as "function creep" and are adamant that society must guard against it occurring in the realm of biometrics, suggesting that it may be one of the biggest impediments to widespread biometric adoption considering current practices of information sharing among firms and between firms and governments. Such a situation developed in Texas after the installation of wireless technology in police cars (Nunn 1994). Previous to this capability, officers were required to radio their dispatcher and provide a plausible explanation as to why a license plate should be checked. The new technology allowed officers to check license plates on a whim, which they freely admitted doing. Furthermore, part of the sales pitch was that it would allow the officers to delve further into the lives of the registered owner as they would link the license plate database with various other databases.

Subsequent to the work done by Smith et al. (1996), Stewart and Segars (2002) empirically confirmed the validity of this model and its fifteen item scale. Extending this research into cyberspace, Malhotra et al. (2004) developed and tested a model that suggested that information privacy for internet users was composed of three dimensions: collection, control, and awareness of privacy practices. While privacy has always been a concern for consumers and a topic of interest for researchers across a broad spectrum of disciplines (Sheng et al. 2006), it is only recently with the advent of mass storage media and the internet that it has attracted the attention of information technology academics (Dinev and Hart 2006; Sheng et al. 2006). Privacy concerns have been demonstrated to have a negative affect on trust (Van Dyke et al. 2007; Malhotra et al. 2004) and the use of the internet as a purchase destination (Dinev and Hart 2006). Concerns about privacy have a strong negative effect on purchase intent both directly and through trust (Eastlick et al. 2006). Other studies have concluded that uncertainty regarding the privacy and security of transaction information make users reluctant to purchase online and that privacy has a significant impact upon the level of trust a consumer has for an e-vendor (Liu et al. 2004).

Control is seen as "central to the concept of privacy." (Van Dyke et al. p. 68) This position is also held by Westin (1967) and Fried (1984). "Privacy is not simply an absence of information about us in the minds of others, rather it is the *control* we have over information about ourselves" (Fried 1984, p. 209). Information privacy may be defined as the right that individually identifiable information not be disseminated to other individuals or organizations; however, in cases where personal information is held by another party, the individual should be able to exert substantial control over both the data and its use (Clarke 1999). Although a recent survey suggests that the public considers privacy to be a complex concept, there seems to be overwhelming agreement with academics as over 90% of the respondents defined "privacy as ownership and control of personal information." (Acquisti and Grossklags 2005, p. 28)

Culnan (1993) demonstrated that "control emerges as a clear theme in differentiating individuals with positive overall attitudes toward secondary information use from those with negative attitudes" (Culnan 1993, p.341). While this research was done in the context of shopping by mail and the ability of mail order companies to gather significant amounts of consumer information, more recent research has been aimed at this concept within the realm of e-commerce (Chen and Barnes 2007; Van Dyke et al. 2007; Flavián and Guinalíu 2006; Hampton-Sosa and Koufaris 2005; Olivero and Lunt 2004; Koufaris 2002) given the ability of companies within this trade channel to collect and store massive amounts of data on their customers.

In their qualitative study, Olivero and Lunt (2004) suggest that consumers are beginning to realize the market value of information about themselves. This creates a perception of increased risk when sharing their data. This, in turn, results in the demand that consumers be more involved in the decisions as to when and to whom their information is released. "More specifically, the demand for active control indicated the need for instruments that can allow consumers to take informed decisions in the exchanges with companies and trade appropriate benefits. By providing this type of control, firms can still aim at establishing successful relationships with customers, although more based upon cooperation and less on trust." (Olivero and Lunt 2004, p. 260)

As mentioned previously, various authors see control of personal information as a core concept of privacy (Clarke 1999; Fried 1984; Westin 1967). Singh (2006) sees it as a lynchpin connecting a variety of interrelated constructs. "[The] control of personal information connects security, trust, privacy, and identity." (Singh 2006, p. 74) Others have segregated it as a distinct construct. For example, Dinev and Hart (2004) demonstrated that perceived ability to control information is different from perceived privacy concerns. Van Dyke et al. (2007) demonstrated that a new construct (perceived privacy empowerment) was separate from, and had a negative effect upon, privacy concerns. There are a variety of divergent views of where control, and/or empowerment lies in relation to privacy. Perhaps this is due to the relative newness of the proliferation of information proffered by technology such that, over time, a more generally accepted

view of informational control and where it fits will emerge. Regardless of whether or not this occurs, the various divergent views on the subject imply that considerably more research is required.

2.3.6.2 Security

The literature appears to address the issue of privacy more than that of security. As discussed previously, this may be due to the complexity of defining exactly what is meant by privacy. Nonetheless, as various high profile security breaches are being extensively covered in the media, the concept of security, and consumers' attitudes towards it, seems to be coming more to the fore (Chen and Barnes 2007; Flavián and Guinalíu 2006; James et al. 2006; Zhang et al. 2006; Joines et al. 2003; Park and Kim 2003). Some of these articles (Chen and Barnes 2007; Flavián and Guinalíu 2006; James et al. 2006) tend to look at security in conjunction with privacy as security breaches typically imply a loss of privacy. Even within the narrower focus of privacy being defined as control over one's information, the unauthorized access or theft of the latter entails a loss of individual control.

Unfortunately for researchers, the intermingling of the terms "privacy" and "security" has resulted in confusion in the minds of consumers (Yousafzai et al. 2006). This phenomenon has been further exacerbated by legislators and companies (Flavián and Guinalíu 2006) and researchers themselves. For example, of the seven items Korgaonkar and Wolin (1999) identified as being either motivations or concerns in using the Web, one was transaction-based security and one was non-transactional privacy concerns. Extending this conglomerate definition, Joines et al. hypothesized that "shopping online will be negatively and significantly related to transaction-based security and privacy concerns" (Joines et al. 2003, p. 96).

Flavián and Guinalíu (2006) see the concepts of privacy and security as separate but highly interrelated. "Privacy is linked to a set of legal requirements and good practices with regard to the handling of personal data...Security refers to the technical guarantees that ensure that the legal requirements and good practices with regard to privacy will be effectively met. For example, the company may promise that the data will not the given to third parties without the consumer's consent. Yet hackers might get hold of the data and hand them over to malefactors. This invasion of privacy can only be prevented by the use of suitable security measures." (Flavián and Guinalíu 2006, p.604)

Despite acknowledging that privacy and security are two distinct concepts, Flavián and Guinalíu (2006) suggest that they should be combined to form one overarching construct: perceived Security in the Handling of Private Data (SHPD). The basis for this combination is that, first, there is often not a clear distinction within the minds of consumers, arguing that it is not relevant to them. Their concern is that they simply want their private information protected; the security measures employed are an issue for the organization. Second, organizations also seldom make a distinction between the two; they view privacy protection as being dependant on behavioural guidelines

and/or the law, as well as the reliability/security of information systems. Finally, lawmakers and public oversight organizations look at policies and procedural issues concerning private data as well as issues "of a purely technical nature (e.g. Directive 2002/58/EC of the European Parliament and of the Council, of 12th June 2002 (European Commission 2002), concerning the processing of personal data and the protection of privacy in the electronics communication sector)" (Flavián and Guinalíu 2006, p. 605).

Chen and Barnes (2007) examined the effect of perceived security and perceived privacy on initial trust in the online environment. While their hypotheses that perceived security and perceived privacy do have a positive effect upon online initial trust was supported, it may be argued that their research instrument was flawed. First, while they based their research upon the model proposed by Yousafzai et al. (2006), the latter was a concept paper such that the authors did not develop, yet alone validate, any survey instrument. Therefore, further testing and possible refinement of the instrument is required. In conjunction with this weakness, the authors defined perceived security in the context of protection from economic hardship and perceived privacy in the context of consumer control of personal information. While the questions posed regarding perceived security seem to fit within the definition they provide, two of the five questions posed regarding perceived privacy do not. Specifically, they ask "the personal information that I provide on this website is secure, [and] the monetary information that I provide on this website is well protected" (Chen and Barnes 2007, p. 35). Neither of these questions goes to the privacy concept of consumer control; but both of them go to the concept of security, with one actually using the term "secure". This example is simply meant to 1) stress the need for consistency between the definition of the construct being investigated and the questions posed; and 2) demonstrate how research may inadvertently further cloud the distinction between the interrelated but separate concepts of security and privacy.

Drawing on research done by Bailey and Pearson (1983), Park and Kim (2003) examined the effect of consumers' security perception upon commitment to a website and, ultimately, purchase behaviour as mediated through information satisfaction and relational benefit. They defined security perception as "customer perceptions about the ability of an online store's controlling and safeguarding of transaction data from misappropriation or unauthorized alteration" (Park and Kim 2003, p. 27). They hypothesized that there would be a positive relationship between security perception and both information satisfaction and relational benefit. Their findings supported their hypotheses.

Previously, research has looked at consumer concerns about website usage with privacy and/or security concerns often being cited by customers (Miyazaki and Fernandez 2001; Miyazaki and Fernandez 2000; Korgoanakar and Wolin 1999). Subsequent research has explored the relationship between privacy concerns and/or security concerns on trust, loyalty, satisfaction, intention to adopt, etc. In this research, privacy and security have typically been in relation to a given context such as mail order services or websites.

2.3.7 Privacy and Security and Perceived Usefulness

While consumers would like personalized products and services, they want them by providing as little information as possible (Adomavicius and Tuzhilin 2005; Murthi and Sarkar 2003). The reason for this trepidation on the part of the consumer is that, while personalization does have benefits, it also requires relinquishing personal information thereby raising privacy concerns (Van Dyke et al. 2007; Flavián and Guinalíu 2006; Roussos et al. 2003; Culnan and Armstrong 1999; Culnan 1993). The result is the "personalization-privacy paradox" (Awad and Krishnan 2006).

Dinev and Hart (2006) and Dinev et al. (2006) suggest that a consumer's decision as to whether or not to release personal information is driven by a rational appraisal of two sets of contradictory factors. Most models investigating e-commerce adoption have looked at "the relative strength of noncontrary factors (e.g. shopping convenience, ecology concerns, customer relationships, and product value)" (Dinev and Hart 2006, p. 62; Torkzadeh and Dhillon 2002). Laufer and Wolfe (1977) suggest that, when deciding whether or not to disclose personal information, individuals take into account such things as "institutional norms of appropriate behaviour, anticipated benefits, and unpredictable consequences" (Dinev and Hart 2006, p. 62) which are at least in part determined by personal beliefs. Culnan and Armstrong (1999) extended this reasoning and noted that consumers engage in a decision process they refer to as a "privacy calculus" and that individuals are more willing to disclose information if they are informed of how a business will handle personal information and perceive the organization to be fair. Subsequently, Culnan and Bies (2003) likened an individual's privacy calculus to an internalized cost-benefit analysis in which the individual will disclose personal information if the benefits received from doing so will at least equal, but hopefully surpass, their assessment of the risk of disclosure. "A positive net outcome should mean that people are more likely to accept the loss of privacy that accompanies any disclosure of personal information as long as an acceptable level of risk accompanies the benefits" (Culnan and Bies 2003, p. 327).

Research by Sheng et al. (2006) demonstrated that "customers' perceived benefits are seven and a half times more influential on customers' adoption intentions than their privacy concerns." (Sheng et al. p. 28) While these findings are considerably higher than those reported by Chellappa and Sin (2005), who found that personalization is two times more influential than privacy concerns, they are directionally the same. One possible explanation put forward by Sheng et al. (2006) was that their subjects were relatively young (below 38) and, per Sheehan (2002), younger people tend to be more pragmatic in terms of sacrificing privacy for benefits. Extending the work of Culnan and Armstrong (1999) and Culnan and Bies (2003), Dinev and Hart (2006) and Dinev et al. (2006) suggest that the consumer simultaneously evaluates two sets of contrary factors: inhibitors, such as internet privacy concerns and perceived risk, and positive drivers, such as trust and perceived control over the personal information they share. While the influence of one belief might override another, it does not eliminate its importance.

While the research done by Sheng et al. (2006) was within the realm of ubiquitous commerce (u-commerce), or "anytime, anywhere" commerce, it may be extended to e-commerce where consumers are willing to give up personal information for the benefit of convenience, for example. In other words, a consumer may be willing to share highly personal information such as a credit card number and their address in exchange for the "convenience" of shopping online, or possibly more appropriately, avoiding the inconvenience of driving back and forth to the mall, searching for a gift, standing in line to pay, etc. This could be more accurately described as a "convenience-privacy paradox".

Continuing along this vein, perhaps this paradox also exists within the concept of security. Research done by Zhang et al. (2006) did not address this issue explicitly. Nonetheless, it is noteworthy that the effect of perceived convenience was almost five times as strong as the effect of perceived security on user satisfaction with e-services which, in turn, had a very strong effect on intention to use e-services. As with Sheng et al. (2006), the respondents in the study done by Zhang et al. (2006) were relatively young with 93% being below the age of 36.

Although the study by Singh (2006) was qualitative, similar results were noted. Almost 80% of the small sample interviewed "valued [the] convenience and habit [of internet banking] over concerns about privacy and security" (Singh 2006, p.76). The anecdotal evidence suggests that some people do take some measures to protect themselves, such as using credit cards with low limits, keeping passwords secure, and only using secure websites. However, in conjunction with these findings were admissions of not understanding the technology and the belief that they would one day be the victims of fraud due to their online banking activities; with this also came the belief that the banks system was "secure" and that, should there be a monetary loss, the bank would reimburse them.

The finding that the technical aspects of security, while important, are lost upon most users (Singh 2006), was also observed by D'Hertefelt (2000). In doing qualitative research to make a European airline's site more user-friendly, it was noted that technical issues such as encryption, authentication, digital certificates, etc. were not that important. The perception of security was enhanced by the simplicity of the site and the availability of user support.

Perhaps the personalization/convenience-privacy/security paradox occurs as a result of cognitive overload. This phenomenon is demonstrated by Acquisti and Grossklags (2005). Their research demonstrated non-optimal behaviour where respondents seemed more than willing to give up long term privacy exposure for short term benefits, even with "perfect" information. This is known as time-inconsistent discounting (O'Donoghue and Rabin 2000) and implies that "people have a systematic bias to overrate the present over the future" (Acquisti and Grossklags 2005, p. 31). The authors attribute this behaviour to humans' inability to process large amounts of complex

data and reach a true optimal decision. "Especially in the presence of complex, ramified consequences associated with the protection or release of personal information, our innate *bounded rationality* (Simon 1982) limits our ability to acquire, memorize and process all relevant information, and it makes us rely on simplified mental models, approximate strategies, and heuristics." (Acquisti and Grossklags 2005, p. 27) Regardless of the underlying thought process, or lack thereof, there appears to be willingness on the part of the consumer to part with personal information in exchange for perceived benefits, be they rewards, personalization, or convenience.

2.3.8 Context of Technology Use

Consumer behaviour research examining the impact of context is not new (Cote et al. 1985; Belk; 1975; Belk 1974). In one study, looking at food preferences, almost half of the explained variance was attributable to situational effects (Belk 1974). Furthermore, situation dependency affects not only consumer preferences but also the way they interpret relevant information (Grewal et al. 1996).

Within technology acceptance research, investigating the significance of context is a relatively more recent development (Yoon and Kim 2007; James et al. 2006; Sheng et al. 2006; Gehrt and Yan 2004; Malhotra et al. 2004; Monsuwé et al. 2004). "The value of a specific technology to a particular customer varies according to the context in which the technology is used. In general, context refers to the situation and environment in which humans perform their activities (therefore, situation and context can be used interchangeably). More specifically, context provides an understanding of the way and circumstance an activity is being performed (Basole 2004). Because a user's concerns and needs vary with the context in which he/she uses the applications, the services that can meet the user's needs in a specific context will provide the best value for the user. Such phenomenon is called 'situation dependency' (Figge 2004)." (Sheng et al. p.8)

Monsuwé et al. (2004) suggest that there is a wide variety of situational factors that should be taken into account in order to develop a fuller understanding of consumers' motivations for using the internet as a shopping channel. In their literature review examining what drives consumers to shop online, they discussed five: 1) time pressure, which is described by Wolfinbarger and Gilly (2001) as convenience and accessibility; 2) lack of mobility (Avery 1996); 3) geographical distance; 4) the need for special items (Wolfinbarger and Gilly 2001); and 5) attractiveness of alternatives.

In the development of their model of Internet Users' Information Privacy Concerns (IUIPC), Malhotra et al. (2004) examined the effect of various contexts. The type of information asked (i.e. more sensitive versus less sensitive) had a significant impact upon behavioural intention and its antecedents of trusting beliefs and risk beliefs. Internet experience and media exposure (how much respondents heard about the misuse of information collected via the internet) also affected the result; but experience as a victim of an improper invasion of privacy did not. In terms of looking at future research,

Malhotra et al. (2004) "contend that consumers' reactions to a specific privacy threat are highly dependant on contextual factors". (Malhotra et al. 2004, p. 350)

Within the domain of ubiquitous commerce, Sheng et al. (2006) investigated the context of emergency versus non-emergency situations upon the effect of personalization on privacy concerns. Their results demonstrated that "customers are more concerned about their privacy when emergencies are not expected than when emergencies are expected". (Sheng et al. 2006 p. 24)

Within the work environment, a number of researchers have examined the influence of voluntariness upon technology adoption (Venkatesh et al. 2003; Karahanna et al. 1999; Agarwal and Prasad 1997; Hartwick and Barki 1994). While some authors have demonstrated its moderating influence (Venkatesh et al. 2003), others have shown that it can have a direct effect upon behavioural intention (Karahanna et al. 1999) and attitude (Moore 1989).

2.3.9 Summary

The original TAM has been though multiple iterations and modifications as researchers attempt to identify more constructs and contexts that contribute to, or detract from, an individual's behavioural intention to use technology. Various avenues explored include e-commerce and m-commerce and additional constructs include playfulness and various aspects of trust. The research by James et al. (2006) extended TAM into the realm of biometric acceptance. However, given that the latter paper is one of the first to explore the factors influencing acceptance of biometrics, it too is but a first step. As the authors state, "the purpose of the study was not to determine which context or device types impacted the attitudes of the users, rather to develop a generalizable model of technology acceptance for this category of devices." (James et al. 2006, p. 11) In addition, their research focused more on general behavioural traits as antecedents to acceptance and did not consider mediating situational variables. Therefore, there is considerable research left to be done to investigate various contexts such as type of individual (i.e. customer versus employee), type of application (i.e. admittance to a theme park as a season ticket holder versus accessing one's bank account), type of device (i.e. fingerprint versus retinal scan), control (i.e. the organization maintains the biometric template versus the individual retaining it on a smart card), and whether or not the program is voluntary.

Chapter 3 Research Model

As has been previously discussed, there is an abundance of research regarding technology acceptance from a variety of viewpoints such as new software, mobile commerce, electronic commerce, and ubiquitous computing. However, it appears that the literature is bereft in terms of looking at technology acceptance in terms of biometrics. Despite an extensive search, only one article was found that extended the Technology Acceptance Model (TAM) into the realm of the intention to use biometric devices (James et al. 2006). Additional articles (Moody 2006; Eschenburg et al. 2005) were found that looked at the acceptability of various biometric identity authentication methods, but they did not examine antecedents to acceptability, or extend into the contexts, that could have an impact upon an individual's willingness to use biometrics.

Also, while there is a vast array of articles that examine the privacy and security implications of biometrics, they centre upon the overarching societal, public policy, and national security implications as opposed to the much more micro aspects of individual acceptance or rejection of biometric initiatives within the realm of commercial applications (Grijpink 2001). The website of the International Biometrics Group (IBG) lists a plethora of articles. However, they are essentially focused on the technical side of biometrics as the technology strives to keep up with the existing and future demands to constantly lower the False Rejection Rate (FRR) and False Acceptance Rate (FAR), and make the devices more user-friendly and less expensive, etc.

Although this phenomenon implies that there is a significant academic void that needs to be filled, given the dearth of research of consumer acceptability of biometrics, this also means that there is a coinciding lack of biometric-specific constructs and associated validated research instruments. As a result, the only recourse available is to identify very closely related constructs and measures within the realm of e-commerce, m-commerce, and u-commerce and adapt them as necessary being ever vigilant to ensure that the instruments do, in fact, measure the underlying construct. As with all research, this will be an iterative and lengthy process as measurement instruments are continuously fine-tuned, biometric-specific research becomes more robust, and more parsimonious models are developed.

This chapter discusses the various stages of the development of the proposed research model. First, the importance of context within the realm of biometrics is discussed as an introduction to the qualitative research that was conducted with Canadian banks to help determine what they felt might influence consumer perceptions about the acceptability of using biometric authentication. Next, further qualitative research was carried out to elicit any privacy and security concerns that may have been overlooked during the literature review (Straub et al. 2004). Finally, a proposed research model is presented and hypotheses developed.

3.1 The Importance of Context

With the emergence of biometrics, researchers have indeed begun to look at context in terms of public/consumer acceptability. Research published in Biometric Technology Today looked at the acceptability of various applications. The survey was done in Finland, Germany and Spain, and while there were differences among the countries, there was also significant agreement in a few areas (Eschenburg et al. 2005). In terms of overall results, respondents were heavily in favour of using biometrics within the context of ATM access, crossing the border, and traveling by plane. The latter two applications are areas where security is typically high. The ATM application is one where remembering a PIN is usually required; perhaps this result suggests that the underlying motivation is convenience and/or security. One interesting result was that the use of biometric identification when traveling by train was significantly more acceptable among Spanish passengers than it was for either German or Finnish passengers. This is notable as the survey was conducted approximately three months after the terrorist attacks at the Madrid train station (Eschenburg et al. 2005). This suggests that the inclusion of contexts, such as media exposure, debit and/or credit card fraud victimization, etc., as espoused by Malhotra et al. (2004), would have some merit; as would the acknowledgement of the potential bias due to recency effects.

Moody (2006) looked at the acceptability of different biometrics in different situations. In terms of using biometric authentication at an ATM versus using it to access one's office, there was virtually no difference in the acceptability of fingerprints. However, iris scans were found to be much more acceptable at an ATM than to access one's office (approximately 65 respondents versus approximately 38), as were retinal scans (roughly 100 respondents versus 62). Conversely, voice recognition was found to be more acceptable at the office than at an ATM (approximately 88 respondents versus 38).

In looking at the acceptability of biometric authentication methods, James et al. (2006) employed a series of eight scenarios in their research. The scenarios looked at various types (e.g. fingerprint, retinal scan, etc.) and applications (e.g. ATM, access to a highly secure R&D area, etc.) of biometrics. While the purpose of the vignettes was simply to investigate a broad spectrum of types and applications to make their results more generalisable to the acceptance of biometrics as a whole, two noticeable findings were tangentially uncovered. First, the use of biometric devices in a public venue met with some reticence (application context), and second, so did the use of retinal scans (type context) (James et al. 2006). The authors also highlight the importance of context given the plethora of applications in which biometrics can be used. "Unlike many traditional technologies, [biometrics] are not specialized in their usage setting or purpose and their usefulness is often associated with their function rather than their stand-alone implementation, as would be the case with a software package. Biometric devices may be adopted for use in a variety of settings for a myriad of functions for different types of entities." (James et al. 2006, p. 4)

3.2 Preliminary Qualitative Research – Banks

In their attempt to thwart fraud, Canadian banks are exploring a variety of avenues. Part of the impetus behind this initiative is the fact that Canadian banks typically reimburse customers for any direct financial loses associated with fraud, again be it skimming a debit card or stealing a credit card, etc. To this end, four of the five major banks joined the ORNEC consortium (Ontario Research Network for Electronic Commerce) to assist in reviewing the problem and investigate various ways of at least reducing the problem as they realize that it is unlikely that it will ever be completely eradicated.

In addition to the banks, the consortium consisted of representatives from various governmental and police organizations, as well as researchers from various Canadian universities. Bank representation typically came from those areas responsible for privacy and/or security. Several meetings were held to assess the prevalence of identity fraud and discuss various alternatives to mitigate its occurrence. One of the areas of interest that came out of these discussions was the use of biometrics for customer identity authentication. Therefore, individual meetings, with personnel responsibility for privacy and/or security at the four banks, were suggested as a method to supplement the information gathered from the literature review.

Semi-structured exploratory interviews were conducted to establish which variables are most salient for consumer acceptance of biometric technology in the financial industry. When selecting interviewees, purposive sampling was used as outlined in Erlandson et al. (1993) to insure reasonable representation from subject matter experts. This resulted in the identification of one individual from each of the four banks to be interviewed. As recommended by Miles and Huberman (1994), interviews continued as long as unique contributors were being identified. In this case conceptual saturation occurred quickly, after only 3 interviews. This was not surprising due to the high levels of industry communication, shared policies, and relative homogeneity within the Canadian banking industry. One interview was done via phone and two were done in person. The phone interview lasted approximately 45 minutes while the in-person interviews went longer and took approximately 75 minutes.

Cognitive interviewing techniques were used to minimize interviewer bias as recommended by Willis (1999). This included the "think aloud" technique outlined in Willis (1999), which encourages respondents to verbalize their thought processes as they respond to the questions. This technique allows a more sophisticated understanding of complex issues to emerge as the interviewer is exposed to the interviewee's reasoning, not simply their responses. The interviewer also paraphrased the responses throughout the interviews to ensure correct interpretations of respondent's statements were made.

Initial interview questions included the following:

1. Does your bank have a vision and/or plan regarding biometrics?
2. Do you believe that vision is shared by other banks and financial institutions?
3. Do you think customers are satisfied with the existing level of security offered by financial institutions?
4. What would your bank like to know with respect to people's perceptions of biometrics?
5. Do you see any issues that might impede biometric adoption within the Canadian banking industry?
6. In what contexts, scenarios, or applications would you like to examine consumer acceptability of biometric authentication technology?

As recommended by Miles and Huberman (1994), data analysis was conducted after each interview, allowing questions to change over time in response to emerging categories. Data categorization and descriptive and pattern-based coding were used.

The results of the interviews with the bank employees are laid out as follows. Table 3-1 lists the results of the initial discussion with the three bank representatives in order of the points raised. Table 3-2 lists possible contexts that the bank employees felt it would be worthwhile examining as context was envisioned as being an influencing factor in consumer perceptions about biometric identity authentication technology. For those contexts that they felt were worthy of exploring, they were also asked to rank them in order of importance; this ranking is provided in the table.

Table 3-1: Key Insights Provided by Bank Personnel

Bank #1	
1.	Unlikely to be pursued unilaterally by their bank, or any other Canadian bank.
2.	Banks need to collectively assess the tradeoffs between consumer perceptions, cost, and the level of security biometrics provide their customers.
3.	In terms of customer perceptions, where does their responsibility for security end and the banks' begin?
4.	What do customers see as the key benefits and drawbacks of using biometrics?
5.	Do people understand biometrics?
6.	Voice recognition biometrics are already being used for telephone banking, but this is not considered a "high" security application.
Bank #2	
1.	Unlikely to be pursued unilaterally by their bank, or any other Canadian bank.
2.	In terms of customer perceptions, where does their responsibility for security end and the banks' begin?
3.	Do people understand biometrics?
4.	What do customers see as the key benefits and drawbacks of using biometrics?

Bank #3	
1.	Wonders if biometrics is a solution in search of a problem.
2.	Unlikely to be pursued unilaterally by their bank, or any other Canadian bank.
3.	In terms of customer perceptions, where does their responsibility for security end and the banks' begin?
4.	Interoperability concerns.
5.	Do people understand biometrics?
6.	What do customers see as the key benefits and drawbacks of using biometrics?
7.	Will the introduction of chip technology on credit cards confuse consumers and, as such, confound the results of the survey?

Table 3-1 shows considerable consistency in terms of how Canadian banks view biometrics in general. Given the nature of the Canadian banking industry, it was unanimous that biometrics was viewed as something that would be pursued by all the banks or none of the banks. This was due to two considerations.

First, there are five major Canadian banks that collectively have a significant share of the consumer banking market but that individually do not have enough clout to be market leaders. Therefore, if any one of them unilaterally decided to pursue customer identity authentication via biometrics and it was not well received, it could cost them market share and the associated profits; and this would be in addition to the substantial upfront costs of installing the technology. Even if it was embraced by customers such that it created initial competitive advantage, this would not be sustainable simply because the technology is widely available and, hence, could be easily replicated relatively quickly by the other four banks. However, if the five Canadian banks deemed that it was in their best interests, most likely from a cost-benefit perspective, to introduce biometrics and collectively agreed to do so at approximately the same time, this would mitigate the possibility of any major redistribution of market share should there be consumer backlash simply because of the limited options available to the Canadian consumer.

The other consideration as to why Canadian banks would pursue it collectively is due to the existing technological infrastructure with respect to debit cards. While the initial rollout of identity authentication using biometrics would be at bank ATMs, the feeling is that it would inevitably become more widespread such that it would be used essentially wherever you use a debit card. Given this envisioned pervasiveness, banks would have to involve those companies (e.g. Interac) that control the debit card industry and the associated protocols. Again, from both a cost-benefit and competitive standpoint, this is yet another impediment making it unlikely that any Canadian bank would initiate biometric identity authentication individually.

Examining other general discussion points, all three interviewees wondered what people thought with respect to where a customer's responsibility for security ended, and the bank's responsibility began. As the focus of this research was acceptability of

biometrics for identity authentication, this issue was not addressed given the difficulty of operationalising this concept.

The other common concern was whether or not people would understand what was meant by the term "biometrics". In order to address this concern, there would be appropriate wording in the questionnaire defining the term.

Looking at the potential contexts in Table 3-2, there was a good degree of consistency in terms of what were perceived to be the most relevant contexts to examine, and unanimous agreement on the ranking of the top two contexts: voluntariness and control. The importance of whether using biometrics should be voluntary or not is relatively self-explanatory. As mentioned previously, all bank personnel were of the opinion that either the five biggest Canadian banks would adopt biometric identity authentication, or none of them would. Given this statement, combined with their collective market share and a lack of viable options for the Canadian consumer, one might wonder why they would consider voluntariness an issue. The answer is basic customer service. If consumers don't want, or worse are opposed to, biometric identity authentication, than why pursue it, especially given the implementation costs involved. Granted, with only five major banks, the Canadian banking industry gives consumers limited options presently, but that doesn't mean other institutions (i.e. credit unions and smaller banks) won't try to take advantage of any significant customer backlash. Whether or not customers would pursue alternatives (i.e. smaller banks or credit unions) simply due to being forced to use biometrics is debatable, but these smaller market players would inevitably try to leverage any customer discontent to their advantage.

Table 3-2: Ranking of Possible Contexts to Consider in Examining Consumer Perceptions of Biometric Authentication Technology as Identified by Bank Personnel

	Ranking		
Possible Context	**Bank #1**	**Bank #2**	**Bank #3**
Voluntary versus involuntary	1	1	1
Bank control versus shared control	2	2	2
Type of application (debit card, credit card, etc.)	3	3	
Online use versus ATM use versus POS use			3
Type of biometric	4	4	
Safety deposit boxes	5		4
Applicable only to new customers	6	5	5

In terms of control, this was framed in terms of where the biometric information is stored. Bank control means it is centrally stored by the bank. Shared control means that only a portion of the information is centrally stored by the bank, and the remainder is stored on a "smart card" retained by the customer. In the latter case, the information stored at the bank is useless without being combined with the information from the card,

and vice versa. What this means in terms of a consumer's privacy calculus is that while the benefit of convenience is lessened (i.e. the consumer still doesn't need a password, but they now require the card), the "cost" of privacy and security also drops (i.e. the information stored by the bank is incomplete and, therefore, useless regardless of whether it is shared or stolen). While the bank personnel viewed this as key given people's reticence towards the amount of information being captured in general, and by banks in particular, it also aligns well with the conception that the issue of control is central to consumers' privacy perceptions as previously discussed.

Beyond these two issues, type of biometric and application (i.e. debit cards versus credit cards) were deemed areas worthy of investigation by two respondents, while one interviewee suggested that it would be interesting to examine whether there would be any difference based upon ATM use versus online use versus POS (point-of-sale) use. Interestingly enough, no one saw the importance of testing the acceptance of multi-modal (i.e. two or more biometrics, biometric and a password, etc.) authentication methods as they did not foresee that as being offered by the banks.

Two of the interviewees thought examining the acceptability of biometrics within the context of safety deposit boxes would be worthwhile as they envisioned the initial use, or testing, of biometrics potentially being to access safety deposit boxes. This was based upon the premise that, on average, people tend to keep highly valuable assets (be they financial or nonfinancial) in safety deposit boxes, combined with the fact that they are typically used infrequently. The latter point often leads to lost keys and/or forgotten passwords; standalone biometrics (i.e. no shared control with a smart card) would address these problems quite well. Despite the above positive aspects of looking at this application, it was dropped due to the fact that considerably more people tend to have debit cards and use ATMs versus having safety deposit boxes. Ultimately, the aspects of voluntariness and control were the top two choices among the three interviewees and, as such, were the ones chosen for investigation.

Looking at demographics, all three bank employees identified age, gender, income level, and education as being worthwhile to examine. The former two align with previous research as age and gender have been shown to impact technology adoption. Income level was considered salient as it is presumed that people with higher income would typically have more financial assets available via debit cards. As such, they may be more amenable to the use of what is a more secure method of identity authentication, presuming, again, that their perceived benefits outweigh their perceived concerns/costs. Similarly, people that are more educated may have a better understanding of what biometrics can and can't do which may influence their perceptions.

3.3 Preliminary Qualitative Research – Understanding Perceived Benefits and Concerns

Recall from Chapter 2 that privacy and security concerns and usefulness were discussed as factors that influence the attitudes and/or adoption intentions of consumers

with respect to certain types of technology such as the internet, m-commerce, and u-commerce. Furthermore, the discussions with bank personnel indicated that they would like to know what consumers see as the key benefits and drawbacks of using biometrics. Therefore, given the lack of research with respect to factors influencing biometric adoption, it was deemed necessary to obtain a better understanding of the key perceived benefits and concerns that are top-of-mind for consumers prior to the development of the proposed research model and related hypotheses.

3.3.1 Methodology

Data was gathered via an online survey. A description of fingerprint biometric authentication for ATM transactions was provided and subjects were asked the following three open-ended questions:

1. What do you feel are the benefits/advantages of using biometrics?
2. What concerns do you have using biometrics?
3. Please provide any other comments regarding the use of biometrics.

A total of 367 usable surveys were obtained from across Canada. There was a roughly equal representation from the demographic perspectives of gender and age, the latter ranging from 18 through to over 55. In terms of education, the majority of respondents had at least some college or university education. Looking at income level, approximately half of the respondents made $50,000 or less, while roughly 10% preferred not to answer. All subjects were above 18, used an ATM, and were not employed by financial institutions.

The data was analyzed using a three stage iterative process. In the first stage, respondents' answers to the questions were reviewed and open coding was used to identify shared characteristics and generate initial descriptive categories. The second stage consisted of scrutinizing the initially identified categories and integrating them into more centralized categories. In the final stage, the use of pattern coding allowed the clustering of these centralized categories into overriding themes (Miles and Huberman 1994). While the first and second stages were conducted by one researcher, the final stage was done through meetings and discussion with two other researchers during which the responses were reviewed for consistency and to build consensus.

Answers to the three open-ended questions were copied into a qualitative analysis program called NVivo. After the first and second stage analyses, the following general categories were identified as concerns of using biometric verification in the context of ATM transactions:

1. How secure is my information from hackers/insiders?
2. My fingerprints can be copied.
3. The increased possibility of identity theft.
4. Inconvenience.
5. Inability to share banking responsibilities with others.

6. Reliability of the technology in terms of startup glitches, ongoing maintenance issues, and accuracy of the fingerprint reader due to dirt, grease, etc.
7. Slower access to accounts.
8. What happens if my fingers are damaged, or if they become damaged?
9. What happens when I go overseas and they aren't using biometrics at ATMs?
10. It's too much information for the banks to have.
11. I don't like supplying biometric information to the bank.
12. I am concerned about my privacy.
13. How well will my privacy be protected?
14. Will my biometric information be used for reasons beyond those intended (i.e. shared with other corporations, law enforcement, governmental agencies, etc.)?
15. Physical harm as thieves will now severe my fingers and/or hand to gain access to my account.

The third stage analysis resulted in the synthesis of the twelve concern categories into five recurring themes. They were:

1. Security Concerns (Items 1 through 3)
2. Inconvenience (Items 4 through 9)
3. Privacy Issues (Items 10 through 13)
4. Function Creep (Item 14)
5. Physical Harm (Item 15)

The NVivo analysis revealed the following 13 general benefit categories in the first and second stage analyses:

1. Increased security
2. Increased safety
3. Difficulty in reproduction of fingerprints
4. Deterrent to identity theft
5. I am the only one with access to my accounts
6. Less chance of theft from my accounts
7. Less chance of theft of my PIN/password
8. Less concern if I lose my card
9. Easier to use
10. No chance of forgetting your card
11. No PIN/password to remember
12. Convenience
13. Faster access to accounts

The third stage analysis, again, conducted in conjunction with two other researchers through meetings and discussions, resulted in the synthesis of the thirteen broad benefit categories into two overriding themes due to the sufficient commonality identified among the second stage categories. The two higher level benefit constructs identified were:

1. Increased Security (Items 1 through 8)
2. Convenience (Items 9 through 13)

3.3.2 Results

Looking at Table 3-3, the concerns, ranked by order of number of mentions, are security, inconvenience, function creep, privacy, and physical harm. Security was the greatest concern for people and by a considerable margin as it was cited as an issue by 145 respondents, which represents almost 40% of the usable surveys. Typically, respondents were worried about the ability of thieves to access their biometric data thereby giving them access to their financial information and assets as is exemplified by the following comments: "*Anyone could hack into the system and take information*"; "*If identity theft occurred, it would be far worse than now.*"; "*I have concerns about fingerprints which I think can be copied.*"; "*Somebody somehow getting my fingerprint to access my account.*"; "*Fingerprints left on ATMs may be lifted and used by those who know how.*"; "*Overall security is a concern because there are ways to replicate fingerprints.*"

Table 3-3: Concerns of Using Biometric Authentication at ATMs

Concern	Number of Mentions	Percent of Respondents
Security	145	39.5%
Inconvenience	99	27.0%
Function Creep	81	22.1%
Privacy	77	21.0%
Physical Harm	38	10.4%

Of particular interest was the finding that some people believe that it is the actual biometric that is stored when, in actuality, recall that the biometric is converted into a mathematical expression which is then stored as the template for identity authentication. Currently, it is not possible to reverse engineer a viable biometric from the encrypted mathematical expression.

Inconvenience was the second most cited concern as it was mentioned by 99 people, or 27% of the survey participants. The biggest issue around inconvenience seemed to be the inability to have someone else do your banking for you. Despite bank direction to the contrary, it would appear that some people are in the habit of sharing banking duties with their friends and significant others. Unfortunately, the implementation of biometric authentication would make it impossible for this practice to continue. Presumably, shared accounts will be able to be accessed by either owner providing their fingerprint for authentication, but for those relationships where the parties prefer to have separate bank accounts, this may be a significant hurdle with respect to acceptance. Beyond this aspect, the issues of being incapacitated, startup glitches, and ongoing reliability were also mentioned. Some of the responses within the inconvenience context included: "*Sometimes I give my bank card to my significant other or close friends or relatives to withdraw money or deposit cheques for my business. They would not be*

able to do this."; "*Personally, I allow my fiancée to access my bank account. Whoever has the free time that day takes both cards and paycheques or withdrawals and runs to the bank for us both.*"; "*If I am sick and unable to go to the bank to get money, my partner would not be able to go for me.*"; "*The time it will take to get the system running without any glitches (but it's standard with any new thing)*"; "*The technology is still young and imperfect*"; "*Early models flawed. Quality of biometric reading component, not working*"; "*Could be more complicated, and I have my doubts concerning the reliability of the new system*".

Function creep was mentioned by 81 respondents, which represents just over 22% of the usable surveys. Recall from Section 2.2.1 that function creep refers to the concern that the initial use of biometric-based systems will morph and expand, innocently and/or covertly, into other areas not previously envisioned or agreed to by those enrolled in this type of authentication mechanism (Langenderfer and Linnhoff 2005). Also as previously stated, Langenderfer and Linnhoff (2005) suggest that function creep may be one of the biggest impediments to widespread biometric use due to current information sharing practices amongst for-profit and governmental organizations. In fact, some law enforcement information systems have been sold based upon their ability to assimilate information from an array of various databases (Nunn 1994). Some of the responses were: "*I would not accept this service unless there was legislation in place where NO one else could access this information, including the government.*"; "*Banks releasing my fingerprint to other companies/agencies.*"; "*I am concerned that the info could be made available to the government or any other agency as well.*"; "*Who else will be able to get their hands on this biometrics and use if for other situations?*".

Privacy was close behind function creep as 77 people, or 21% of the survey participants, mentioned it as an issue. Responses included: "*Privacy is important to all of us and by using this we are giving out way to much*"; "*I don't like the idea of someone having that much information about me.*"; "*I don't know that I like the idea of providing my bank with my fingerprint, although not for any definable reason, I just feel that it's very personal.*"; "*Biometrics is more secure but we have to make sure that our privacy and our rights remain protected at all cost.*"; "*I am concerned about misuse of the technology and the potential of loss of privacy.*"

Finally, while the concern that garnered the least number of mentions was the threat of physical harm, it was still mentioned by 38 people, or just over 10% of those surveyed. While there are viability tests to help ensure that the biometric being authenticated is coming from living tissue, this may be of little comfort in the minds of consumers given that the present system just requires one to surrender their debit card and PIN to a would-be thief thus potentially avoiding physical violence more so than when one is dealing with a piece of oneself. Comments with regard to this concern included: "*I fear the crime that might take place against the person. Now if a thief wants access to your account, they simply steal your card even if that means knocking you out for it. In this new scenario, the thief would have to basically kill you to steal your finger.*"; "*I*

would also be concerned about people attacking me, cutting off my finger, and using it to access my account. Then I've lost money and a finger."; "*People cutting off fingers to rob someone.*"; "*Please be aware that criminals will use whatever means they have to in order to steal, and therefore they may cut off fingers to gain access etc.*"; "*Someone cutting your finger off to access your account.*"; "*The Hollywood scenario to cut the finger off to access bank accounts is more probable.*"

In addition to the above findings, another trend was noted that lends support to the notion espoused by Flavián and Guinalíu (2006) that perhaps there is not a clear distinction between privacy and security in the minds of consumers, at least within the context of biometric authentication technology for accessing one's bank accounts. When people discuss privacy and security concerns from this perspective, many of them tend to mention more than one dimension of either privacy, security, or both. Of the 367 respondents, 92, or just over 25%, mentioned both a privacy and a security concern. When multiple mentions of privacy concerns or security concerns are added to this group, the number jumps to 142 participants, or almost 39%. Some of the comments that exemplify this phenomenon are as follows: "*Privacy is important to all of us and by using this we are giving out way too much. In the past people have hacked cards, etc. and if they ever hacked into this it would be a nightmare.*"; "*I would be concerned about the bank having personal material on me, such as my fingerprint, and how this could be used by hackers and police.*"; "*Too much info and not enough safeguards.*"; "*My personal information could be sold, offered, stolen, etc. by, or to, other parties.*"

Moving on to benefits, the findings are summarized in Table 3-4. Increased security was mentioned as a benefit by 203 respondents which equates to just over 55% of the total, while convenience was cited by 97 people or just over 26% of the survey participants. Some of the comments made regarding security were: "*I think in itself it should be more secure because no one has the same fingerprints.*"; "*Less chance of someone else stealing my identity.*"; "*I wouldn't need to worry about someone stealing my PIN number (whether by watching over my shoulder or on security cameras, etc). I'd feel more secure that my money couldn't be accessed as easily.*"; "*I feel that it will increase the security regarding personal banking.*"; "*You feel more secure in knowing that only you can access your bank account, because nobody else has the same fingerprint as you.*"; "*Foolproof identification and protection of my banking transactions.*"; "*It would be another layer of security to protect my identity.*"; "*I think maybe it would be more secure than a bank card because only one person has your fingerprint... YOU!*"

Table 3-4: Benefits of Using Biometric Authentication at ATMs

Benefit	Number of Mentions	Percent of Respondents
Increased Security	203	55.3%
Convenience	97	26.4%

On first glance, it seems odd that security is identified as a benefit by over 55% of the respondents while being simultaneously cited as the primary concern by almost 40%

of the survey participants. However, upon further review of the answers, the respondents appear to be discussing two different points of view. When security is mentioned as a benefit, it is typically within the context of access to financial data (i.e. only I can access my accounts, the bank is sure it is me, etc.). When security is mentioned as a concern, it is typically mentioned within the context of the bank not having appropriate safeguards to protect the biometric data itself. In several cases, respondents mention both contexts in the same sentence saying that it will be a much more secure method of verification for access to financial assets provided the security around the biometric data is sufficient. This is exemplified by the following sample of comments: "*If it could be guaranteed (the security) I would like it very much, because I think in itself it should be more secure because no one has the same fingerprints.*"; "*As long as the other [biometric] information is kept safely at the bank, I believe this is a great security upgrade and will prevent identity theft.*"; "*I know the day is coming, and this would seem to be more secure than a card access with a PIN number. As long as the security of the biometric information can be guaranteed (as much as any security can be), then this would be a great move.*"

A similar phenomenon can be seen in terms inconvenience versus convenience in that 99 respondents, or 27%, mentioned the former as a concern while almost the same number (97 respondents, or just over 26%) mentioned the latter as a benefit. However, unlike security in which it appears that the respondents seem to be discussing two different points of view, in looking at inconvenience and convenience, it seems to be more of a paradox in that participants are looking at opposite sides of the same issue. In other words, if they adopt biometric authentication they will have the convenience of no longer having to use debit cards and PINs, but will have to give up the convenience of being able to get someone to do their banking for them.

Upon further analysis of the micro-level classifications, the convenience benefits are typically: (i) not having to remember a card and/or PIN; (ii) faster service; and (iii) it being easier to use. Remarks made with regard to convenience include: "*No need to have a debit card or [to] remember a password.*"; "*It would be a faster way to access my money.*"; "*You can't forget your fingerprint.*"; "*No pin numbers to remember.*"; "*Fast, convenient, don't have to search for debit card or risk forgetting the PIN.*"; "*No more carrying a card around, don't have to know a PIN, don't have to worry about losing your card.*"; "*It's one less password to forget.*"

3.3.3 Summary

The concerns noted by the survey participants were security, inconvenience, function creep, privacy, and physical harm, while the benefits cited were increased security and convenience. The findings of this preliminary qualitative study investigating perceived benefits and concerns of biometric authentication not only provided additional support for the findings of previous authors, but also informed the development of the proposed research model and related hypotheses. Specifically, within the realm of the Canadian banking sector and the deployment of biometric technology, the concepts of privacy and security concerns appear to be inextricably intertwined in the minds of the

consumer. Moreover, it would appear that consumer attitudes towards biometrics seem to be influenced by a myriad array of both complementary and opposing factors acting simultaneously. This lends credence to the supposition put forward by Dinev and Hart (2006) and Dinev et al. (2006) that the decision to release personal information is determined by the rational assessment of two sets of contradictory factors; and in some cases, these contradictory factors may actually be opposite views of the same factor.

The following sections build upon the findings of both qualitative studies in the following manner. First, the combining of privacy and security concerns into a single construct is discussed; and second, the proposed model is presented and hypotheses developed.

3.4 The Examination of Privacy and Security Concerns as a Formative Construct

As mentioned previously, the terms "privacy" and "security", while distinct, are highly interrelated. Within the context of organizations continuously increasing their ability to accumulate and correlate vast amounts of data, these terms are often mentioned in the same breath when discussing consumers (i.e. what measures are being taken to *secure* customers' *private* information). This situation has been exacerbated by both public policy organizations and private companies as they consistently intermingle the terms. The latter group seldom makes an overt distinction between the two concepts as they look to protect consumer information by establishing sound privacy and security practices (Flavián and Guinalíu 2006). In fact, it may be argued that companies blur the line even further by asking for more and more personal information as a method of increasing security. This is exemplified by the practices of Canadian banks with respect to online banking. They ask one of three personal questions after the customer has signed on using their bank card number and password. The argument is that by relinquishing private information, which is supposedly known only to the account holder, security is enhanced. This example presents a conundrum. Supplying private information increases security; but if that security is breached, one's privacy has been compromised. Subsequently, surrendering additional private information is necessary to re-establish the previous level of security in terms of access to one's bank accounts. Finally, researchers themselves have blurred the line between the two concepts (see Chen and Barnes 2007; Joines et al. 2003; Korgaonkor and Wolin 1999).

Flavián and Guinalíu (2006) address the issue of the consumers' perceived interchangeability of the two terms by developing the construct perceived Security in the Handling of Private Data (SHPD). While acknowledging that privacy and security are separate concepts, the approach suggested by Flavián and Guinalíu (2006) advocates that the semantic distinction is immaterial to consumers and, therefore, these two concepts should be combined when examining their influence. In other words, to the consumer it is irrelevant whether their information was obtained due to a breach stemming from inadequate security or to the sharing of data as a result of lax privacy policies. What is

relevant is the end result: someone, other than those authorized, now has their information.

The use of biometrics as a means of identity authentication is merely an extension of the common online banking practice of asking one of three personal questions; providing private information begets improved security. However, consumers will probably view biometrics as being considerably different when compared to providing a bit of personal trivia. If the answers to one's personal questions become compromised (either by deficient privacy policies or poor security), it is a simple matter of picking different questions and supplying the answers. While this is far from optimal and significant damage could have resulted in the intervening period between the security being compromised and subsequently reinstated, there is no ongoing threat once new questions and answers are supplied by the customer.

The same cannot be said with respect to one's biometric information; if this is compromised, the solution, presuming one exists, will be considerably more complicated. In addition, the damage is more far-reaching since, by its very definition, this is personally identifiable information. As such, in an attempt to increase security by providing very private information, the individual's ongoing security and/or privacy have possibly been broadly and irrevocably compromised. The methodology used to store biometrics makes this scenario virtually impossible given today's technology. However, this may be beside the point in the minds of consumers for a variety of reasons such as not knowing how biometrics work, not knowing how they are stored, a lack of personal exposure to biometrics, how biometrics are portrayed in popular culture, etc. Even if they are versed in biometric technology, they may feel that criminals will ultimately be able to uncover a method of recreating a viable biometric, such as a three-dimensional finger, from the information that is stored. Therefore, given the intermingling of the terms security and privacy combined with the potential implications for both should one's biometrics ever be compromised, not to mention the newness of the technology, it seems reasonable to follow a similar approach to that suggested by Flavián and Guinalíu (2006) and consider privacy and security concerns as a single construct.

The decision to treat privacy and security concerns as a single construct raises the subsequent issue as to whether or not it should be treated as reflective or formative. Formative constructs work differently than reflective constructs. In the former, changes in the measures or items cause changes in the underlying construct whereas in the latter a change in the construct affects the underlying measurement items (Jarvis et al. 2003). As such, in reflective constructs, the direction of causality is from the construct to the items; but in formative constructs the direction of causality is from the items to the construct. There are a variety of formative constructs, typically within the realm of economics (Diamantopoulos and Winklhofer 2001), such as price indices, economic indicators, and socioeconomic status. Looking at socioeconomic status, this is determined from the combination of education, income, occupation, and residence. A change in any one of these items would result in a change to socioeconomic status irrespective of whether or

not the other measures changed; and similarly, a change in any one of the measures does not necessarily affect the other items. Conversely, a change in socioeconomic status does not imply a change in all four measures. Finally, while the four elements of socioeconomic status work independently, there is an element of interconnectedness. For example, while a higher level of education does not guarantee a better occupation and/or income and/or a subsequently better residence, they do tend to influence one another such that there is a degree of correlation amongst the items; but it is not to the same level as the items in a reflective construct. Indicators in reflective constructs are essentially measuring one concept whereas formative constructs are an amalgamation of their indicators.

Based upon the findings of the second study, it appears that consumers are not only unable to distinguish between privacy and security concerns but that they also seem to be worried about some elements more than they are of others. This suggests that, while they have multiple privacy and security concerns, they assign different weights to the various elements, that each element is not addressing the same concern, and that the concerns do not necessarily move with one another, although there may be some interplay among them. Therefore, based upon exhibiting the traits typical of a formative construct, privacy and security concerns was treated as such.

3.5 Proposed Research Model and Hypothesis Development

Based upon the literature review in Chapter 2, combined with the qualitative studies discussed above, a proposed model of consumer acceptance of biometric identity authentication at Canadian banking institutions was developed (Figure 3-1). As stated in the introduction, this research model will be used to address three broad research questions. The purpose of this section is to further refine these overarching questions and develop appropriate hypotheses.

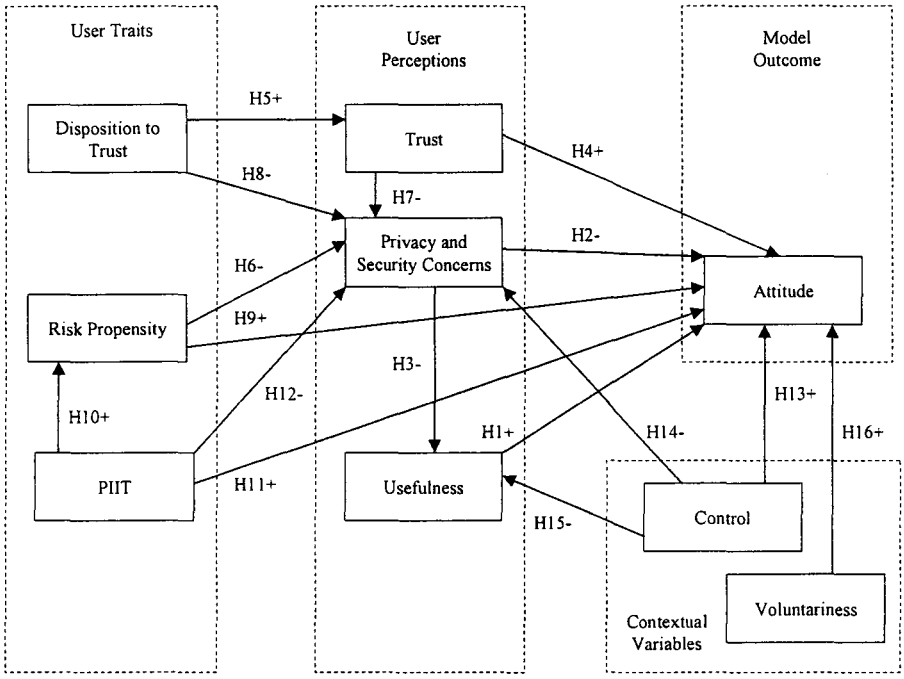


Figure 3-1: Proposed Research Model

3.5.1 Usefulness and Attitude

Recall from Chapter 2 that "attitude refers to an individual's positive or negative feelings about performing the target behaviour" (Chen et al. 2007, p. 302). Furthermore, TAM suggests that perceived usefulness will directly influence attitude. "There is substantial evidence in organizational behavior and management information systems research (e.g. Davis 1989; Davis et al. 1989; Mathieson 1991; Taylor and Todd 1995) suggesting that the key underlying cognition determining an individual's attitude toward the behavior of adopting and using a *new* technology in the workplace is his or her perceptions about the usefulness of the technology" (Venkatesh et al. 2000, p. 36). Path coefficients from perceived usefulness to attitude have ranged from .50 (Davis et al. 1989) to .79 (Taylor and Todd 1995). However, TAM used in isolation appears unable to predict behaviour or provide superior explanations on a consistent basis (Chen et al. 2007; Legris et al. 2003; Venkatesh et al. 2003; Taylor and Todd 1995), possibly because its main thrust was looking at technology acceptance in the workplace. As a result, subsequent researchers have made appropriate adaptations and demonstrated its applicability across various contexts, target populations, and types of technologies (Chen et al. 2007; Gefen and Straub 2003). For example, within the context of electronic toll collection (ETC), Chen et al. (2007) found that the path coefficient from perceived usefulness to attitude was 0.58. Given the considerable research demonstrating the influence of perceived usefulness upon attitude across a variety of technological applications and circumstances, it is reasonable to suggest that perceived usefulness will

also impact one's attitude towards biometric identity authentication technology. Therefore, the following hypothesis is proposed.

> **H1**: Individuals with a higher degree of perceived usefulness will demonstrate a more positive attitude towards adopting biometric authentication technology for accessing their bank account(s).

While perceived usefulness was used in the proposed research model, perceived ease of use was not as it was not considered appropriate for this research. The reason for its omission is simple: the survey participants will be responding to scenarios as opposed to actually using biometric readers such that ease of use will be difficult, if not impossible, to accurately assess. Also, given the wording of the scenarios ("...you must place your index finger on a biometric scanner which instantaneously verifies a match...") the range available for respondents to evaluate ease of use is restricted. In other words, ease of use is controlled for through the scenario description.

Secondly, it may be argued that the respondent may have preconceived notions about certain biometrics in terms of their ease of use, especially when it comes to the invasiveness of certain biometrics such as iris or retinal scanning. However, such "invasive" biometrics will not be included in the scenarios. While this may minimize the ability to generalize the findings to biometrics as a whole, it is merely a reflection of the application that is being investigated. Cost-benefit analysis will be a key consideration in rolling out biometric authentication methods within the banking industry; and given the existing relative cost of iris and retinal scanners when compared to fingerprint readers, and similarly hand geometry readers, the former biometrics are not in the realm of possibility at the present time for bank account access. Obviously, should there be a time when the cost of these two broad biometric authentication measures (i.e. finger/hand versus eye) becomes more on par with each other, then ease of use should be included.

3.5.2 Privacy and Security

Privacy concerns have been studied extensively across a variety of disciplines such as human resources, political science, sociology, psychology, and marketing; however, the interest that information researchers have shown in this area is a more recent development. This relatively new but growing interest has been attributed to the ever increasing pervasiveness of information technology (Dinev and Hart 2006). Companies have always realized the value of being able to track information about existing and potential customers but previously lacked the ability to capture, collate, and react to this information in a cost effective manner. The advent of the information technology age gave companies this capability; and as technology simultaneously advances in sophistication and gets less expensive, this enhances their ability to collect, collate, and cross-reference more and more information. The growth of the internet further augmented the capacity to gather consumer information as it "broadened the extent of data collection [and] improved the capabilities of companies to profile and target specific individuals" (Dinev and Hart 2006, p. 65).

These advances in the capacity to capture data and synthesize it into useful information has resulted in significant benefits to the consumers, such as the ability to more accurately identity preferences and trends, which leads to the development of products and services that better address consumer needs, as well as improved consumer relations (Dinev and Hart 2006; Kling and Allen 1996; Glazer 1991). However, with these benefits comes the concern that too many organizations have too much information about consumers (Dinev and Hart 2006) which is an invasion of privacy (Culnan and Armstrong 1999). Mason (1986) suggests that "the tension between organizational use of personal information and a person's information privacy [is] one of the most important ethical issues of the information age" (Pavlou et al. 2007, p.113).

The disclosing of personal information over the internet increases privacy concerns because the technology creates misgivings in the mind of the consumer it terms of who has access to the information and how it will be used. Furthermore, the more uncertainty the consumer has about these two aspects of the information they provide, the greater will be their privacy concerns (Dinev and Hart 2006). Pavlou et al. (2007) hold a similar view and define information privacy concerns as "a buyer's beliefs about a seller's *inability* and *unwillingness* [italics in original] to protect her personal information from improper use, disclosure to third parties, and secondary use without the buyer's consent" (Pavlou et al. 2007, p.113).

While the accumulation of vast amounts of personal information gives rise to concerns about privacy, the electronic transmission and storage of this information results in concerns regarding security. Over two thirds of Americans are concerned about cyber crime and hackers (McCrohan 2003). Looking at e-commerce, Salisbury et al. (2001) found that perceived usefulness and ease of use had a significantly lower impact upon online purchase intention than perceived information security. In addition, Yang and Jun (2002) demonstrated that concern about security was the most salient factor in deciding not to purchase online. Pavlou et al. (2007) define security concerns "as the buyer's beliefs about a seller's *inability* and *unwillingness* [italics in original] to safeguard their monetary information from security breaches during transmission and storage" (Pavlou et al. 2007, p.113).

Even though the concepts of privacy and security are highly interrelated, they are still semantically distinct. For example, an online retailer, who typically amasses significant amounts of information about their customers, may pride itself upon its record of not experiencing a security breach of any kind while at the same time selling lists detailing their customers' buying and internet surfing habits. In this case, security is strong, but privacy is lax. Conversely, another online vendor may pride itself upon a stellar record of never sharing their customer information with anyone while simultaneously experiencing frequent security breaches. Granted the two situations are not direct opposites in that the lax security in the latter example begets a loss of privacy but the lax privacy in the former example does not result in decreased security. Perhaps it

is these types of nuances between the two concepts that make it unclear in the minds of consumer as to where privacy ends and security begins. Also, people may not attend to the security aspect as they perceive it as too technical (D'Hertefelt 2000) while at the same time believing that their banking information is "secure" (Singh 2006). This confusion is further exacerbated by legislators, academics, and practitioners alike (Flavián and Guinalíu 2006) as previously discussed.

Research shows that security and privacy risks act as deterrents to the adoption of the service of e-banking (Tan and Teo 2000; Bhimani 1996; Cockburn and Wilson 1996), despite the fact that consumers acknowledge the benefits of convenience and time savings (Pew 2002). In addition, consumers are reluctant to adopt new financial products unless it lowers their cost and does not entail changing their behaviour to use it (Barczak et al. 1997). It is likely that consumer perceptions of biometric authentication for financial transactions are similar to those regarding e-banking.

As biometrics are extremely personal by definition, it is reasonable to surmise that consumers will regard the request for biometric information from their financial institution along the same lines as they view the information they are asked to provide to e-vendors. The qualitative research discussed above highlights the privacy and security concerns individuals have regarding the deployment of biometric technology within the Canadian banking industry and how interconnected they are. Furthermore, consumers may consider the present system of debit cards and passwords adequate such that they see biometrics as superfluous. Given that consumers are wary of giving information over the internet, and as biometrics are essentially parts of oneself and therefore highly personal, one can surmise that consumer concerns regarding privacy and security will increase where biometric devices are used. Therefore, the following hypothesis is proposed.

> **H2**: Individuals with a higher degree of privacy and security concerns will demonstrate a less positive attitude towards adopting biometric authentication technology for accessing their bank account(s).

The above addresses the impact of privacy and security concerns upon attitude towards the use of biometric authentication. Perhaps these concerns also have an effect upon perceived usefulness. Featherman and Pavlou (2003) demonstrated that consumer perceptions of risk reduce not only their intention to use the e-service, but also their perceived usefulness of the e-service. As privacy and security concerns relate to the risk that one's biometric information may be compromised, the following hypothesis is proposed.

> **H3**: Individuals with a higher degree of privacy and security concerns will demonstrate a lower degree of perceived usefulness towards biometric authentication technology for accessing their bank account(s).

3.5.3 Trust and Risk

Trust is a belief and beliefs affect behaviour (Ajzen 1991). As previously discussed, trust is a necessity in consumer-marketer relationships (Schurr and Ozanne 1985). Where conditions of uncertainty and ignorance exist regarding the indeterminate actions of others, trust is especially relevant (Gambetta 1990). These conditions exist within the electronic marketplace given its intangible nature relative to bricks and mortar stores (Ba and Pavlou 2002). Essentially, it is the uncertainty inherent in most online transactions that necessitates a higher degree of trust in order for the consumer to use this trade channel. There is a wealth of empirical research suggesting that a heightened perception of trust increases consumer intentions to use an advice website or purchase items from a website (Chen and Barnes 2007; Wakefield and Whitten 2006; Hampton-Sosa and Koufaris 2005; Malhotra et al. 2004; Gefen et al. 2003a; Mukherjee and Nath 2003; Kimery and McCord 2002; McKnight et al. 2002). More specifically, some authors have demonstrated that trust increases one's intention to share personal information with an e-vendor (Bart et al. 2005; McKnight et al. 2002b).

Considering the reticence consumers experience in sharing personal information with e-vendors, one would surmise that the same dissonance could be evoked by their financial institution's request for biometric information as a means of identity authentication. Just as trust is a salient belief when dealing with e-vendors in general, and when sharing personal information in particular, it is reasonable to suggest that trust could also play a significant role in whether or not consumers would be willing to surrender their biometric information in order to access their bank accounts. Based upon the findings of previous authors (see Chapter 2) demonstrating that trust is a key component of the consumer-business relationship combined with its strong direct effect upon intended adoption of e-commerce and other trust related behaviours, this concept is extended into the realm of the acceptance of biometrics as suggested by the following hypothesis.

> **H4**: Individuals with a higher degree of trust in their bank will demonstrate a more positive attitude towards adopting biometric authentication technology for accessing their bank account(s).

The above discussion and hypothesis considers the dimension of trust one demonstrates towards one's bank, or what McKnight et al. (2002) refer to as institutional trust. Various studies have demonstrated that an antecedent to institutional trust is disposition to trust (Kim et al. 2008; Dinev et al. 2006; van der Heijden et al. 2003; Lee and Turban 2001). As the phrases imply, institutional trust is contextual and/or specific to an entity; disposition to trust is a person's tendency to be generally trusting irrespective of specific contexts and/or entities. While disposition to trust is a personality trait and, therefore, relatively stable over time, for each individual it is still nonetheless the interplay amongst a variety of forces, such as experiences, culture, and socialization, that ultimately shapes that person's inherent propensity to trust. "A consumer's disposition to trust is a general inclination to display faith in humanity and to adopt a trusting stance

toward others...This tendency is based not upon experience with or knowledge of a specific trusted party, but is instead the result of ongoing lifelong experiences and socialization." (Kim et al. 2008, p. 552; Gefen 2000; McKnight et al. 1998; Fukuyama 1995; Rotter 1971). After an extensive review of the disposition to trust literature, Das and Teng (2004) concluded that "individuals are viewed as different in terms of their propensity to trust and such differences tend to be robust across situations" (Das and Teng 2004, p. 97).

People with a higher tendency to trust in general typically demonstrate a higher degree of trust in a specific party; conversely, people that have a lower tendency to generally trust are likely to demonstrate a lower degree of trust in a specific entity (Kim et al. 2008; Dinev et al. 2006; Fukuyama 1995; Rotter 1971). Based upon these findings, the following hypothesis is proposed.

> **H5**: Individuals that have a greater disposition to trust will demonstrate a higher degree of trust towards their bank.

Risk propensity has been described as a stable personality trait that has been demonstrated to impact the degree to which an individual perceives risk in a given situation, as well as their behavioural intention. A person with a greater propensity for risk is likely to perceive a situation as less risky than an individual with a lower risk propensity. Similarly, the former individual is more likely to engage in "risky" behaviour than the latter individual.

Bhatnagar et al. (2000) identified information risk, with respect to privacy and security, as being a predominant risk that consumers consider in deciding whether or not to shop online. The concepts of privacy and security concerns as articulated above may be viewed as perceived risks, within the context of using biometrics for identity authentication, in the minds of consumers. As such, perhaps the degree to which a consumer considers these concerns as salient will depend upon their risk propensity. As such, the following hypothesis is proposed.

> **H6**: Individuals with a high risk propensity will demonstrate a lower degree of perceived privacy and security concerns with respect to using biometric authentication technology for accessing their bank account(s).

In their extensive review of the inter-relationship between trust and risk, Das and Teng (2004) give various examples of how trust has been demonstrated to influence risk. As privacy and security concerns constitute a form of perceived risk on the part of the consumer, the following hypothesis is proposed.

> **H7**: Individuals with a higher degree of trust will demonstrate a lower degree of perceived privacy and security concerns with respect to using biometric authentication technology for accessing their bank account(s).

With respect to disposition to trust, McKnight et al. (2002), contend that "*disposition to trust*, [defined in Chapter 2 as a] general propensity to trust others, can also influence an individual's beliefs and intentions towards a Web-based vendor" (p. 336). Within the context of biometric authentication technology usage at ATMs, privacy and security concerns are one's beliefs as to the capability, or lack thereof, of one's bank to address these issues. Therefore, the following hypothesis is proposed.

> **H8**: Individuals that have a greater disposition to trust will demonstrate a lower degree of perceived privacy and security concerns with respect to using biometric authentication technology for accessing their bank account(s).

Prior to Sitkin and Weingart (1995), most research on risk propensity suggested that it had a direct effect upon risky decision-making behaviour. These authors found that this was not the case when risk perception was introduced into the model and instead demonstrated that the effect of risk propensity upon risky decision-making behaviour was fully mediated through risk perception. Subsequent research by Chen and He (2003) did show a direct effect of risk preference upon intention to adopt online shopping even with perceived risk in the model. The definition of risk preference used by Chen and He (2003) is the same as the definition of risk propensity used in this research. Therefore, the following hypothesis is proposed.

> **H9**: Individuals with a high risk propensity will demonstrate a more positive attitude with respect to using biometric authentication technology for accessing their bank account(s).

3.5.4 Personal Innovativeness in the domain of Information Technology (PIIT)

Recall from Chapter 2, Section 2.3.5 that PIIT is "the willingness of an individual to try out any new information technology" (Agarwal and Prasad 1998, p. 206). Rogers (1995) notes that innovators possess certain characteristics. They tend to actively seek information about new ideas and they are less likely to rely on the subjective evaluations of their peers in terms of the consequences of adopting new technology (Agarwal and Prasad 1998). Extending the work of Kirton (1976), who noted that, by definition, innovation is fraught with risk and uncertainty, Rogers (1995) contends that innovators and early adopters are risk lovers. "Insofar as individuals with higher PIIT are more prone to take risks, it is reasonable to expect them to develop more positive intentions toward the use of an innovation, given the same level of perceptions as a less innovative individual. Similarly, for the same level of usage intentions regarding the innovation, the individual with higher PIIT would require fewer positive perceptions than an individual who is less innovative." (Agarwal and Prasad 1998, pp. 207-208)

Hirunyawipada and Paswan (2006) examined "the relationship between consumer innovativeness, perceived risk, and new product adoption" (Hirunyawipada and Paswan 2006, p. 184) within the context of electronics products as they are considered innovative

and high technology goods (Gatignon and Robertson 1991; Rogers 1983). The empirical research done by Agarwal and Prasad (1998) studied the Web as the innovation due to the fact that, at that time, it was an emergent technology and therefore appropriate. Similarly, biometrics is presently an innovative, emergent technology such that PIIT is applicable. Therefore, extending the work of Rogers (1995) and Agarwal and Prasad (1998) with respect to innovators and risk propensity, the following hypothesis is proposed.

> **H10**: Individuals with a high degree of PIIT will demonstrate a higher degree of risk propensity.

Featherman et al. (2006) suggest that "a preference for a 'digital lifestyle' may predispose IT innovators to consider new e-services as similar to other legitimate e-services they have adopted (e.g. preparation and submission of income tax forms)" (Featherman et al. 2006, p. 119). This supposition, combined with the suggestion by Agarwal and Prasad (1998) that consumers with higher levels of PIIT require fewer positive pre-adoption cues than those with lower levels, leads to the following hypothesis.

> **H11**: Individuals with a high degree of PIIT will demonstrate a more positive attitude with respect to using biometric authentication technology for accessing their bank account(s).

Also, given the theorized direct correlation between risk propensity and PIIT as espoused above, as well as the proposed impact of risk propensity upon privacy and security concerns, it seems reasonable to propose the following hypothesis.

> **H12**: Individuals with a high degree of PIIT will demonstrate a lower degree of perceived privacy and security concerns with respect to using biometric authentication technology for accessing their bank account(s).

3.5.5 Control and Voluntariness

As previously discussed, interviews were conducted with personnel from three of the five major Canadian banks. The net effect of these discussions was the identification of control and voluntariness as being key contexts to examine, via the four scenarios, within the context of the broader survey.

Control has been identified as a core element of privacy; and an individual's ability to control their personal information has been demonstrated as a key factor in one's willingness to share it. Within the context of biometrics, one would expect to see the same results, especially given their highly personal and sensitive nature. While it can be hypothesized that the ability to exercise control over ones' personal information will have a positive impact upon people's attitude towards using biometrics, perhaps the influence of control extends beyond just attitude and into the realm of privacy and security concerns and usefulness, two of the direct antecedents of attitude. Given the way

control was operationalised (please see Section 4.1.1), in that the bank only retains half the biometric information and the customer retains the other half on a smart card, it seems reasonable to suggest that this could mitigate some of the privacy and security concerns that consumers may have when compared to the lack of perceived control when their complete biometric information is stored at the bank. Conversely, from the perspective of perceived usefulness, the requirement to now carry a card as opposed to simply placing your finger on a biometric reader may be deemed less convenient. Therefore, the following hypotheses are proposed.

> **H13**: In circumstances where individuals have a higher degree of control over their biometric information, attitude towards the use of this technology for accessing their bank account(s) will be more positive.
> **H14**: In circumstances where individuals have a higher degree of control over their biometric information, privacy and security concerns towards the use of this technology for accessing their bank account(s) will be reduced.
> **H15**: In circumstances where individuals have a higher degree of control over their biometric information, usefulness with respect to the use of this technology for accessing their bank account(s) will be reduced.

While the results from previous research make it seem reasonable to suggest that control will have an impact on attitude as well as privacy and security concerns, and usefulness, the effect of voluntariness is much more speculative. In other words, introducing a voluntary program should intuitively have a positive impact upon attitude; but what effect will it have on privacy and security concerns and usefulness? Unlike control, voluntariness would not seem to have an impact upon privacy and security concerns since voluntariness does not implicitly suggest heightened protocols with respect to privacy and security. Similarly, whether or not the program is voluntary would not appear, in and of itself, to have any discernable impact upon usefulness. Therefore, the following hypothesis is proposed.

> **H16**: In circumstances where biometric identity authentication is voluntary, individuals' attitudes towards the use of this technology for accessing their bank account(s) will be more positive.

Chapter 4 Research Methodology

This chapter describes the research methodology employed to test the validity of the model proposed in Chapter Three. The model was examined through the administration of an online survey in which respondents were asked questions with respect to general personality traits and institutional trust, and then given a specific scenario and asked to answer questions based upon their reactions to that scenario. The following sections detail the methodology and procedures.

4.1 Scenario Research

The typical method for conducting intention adoption is surveys (Webster and Trevino 1995). However, in the case of biometric authentication, most applications are not yet widely used and/or available such that they have not been experienced first hand by consumers. Therefore, scenario-based research is appropriate to examine the proposed model (Sheng et al. 2006).

In scenario-based research, each respondent is presented with a scenario, or scenarios, which vary the factor(s) of interest to the researcher. All respondents then answer the same survey questions. This method is more indirect compared to the traditional survey approach as the importance of factors is inferred based upon individuals' responses to the posed scenarios (Zedeck 1977) as opposed to answering based upon direct experience.

Also, due to the fact that this is a future application (given that biometrics are not widely used in Canada), the scenario method allows the researcher to ascertain which of the contexts examined will have a higher degree of acceptance to consumers (Sheng et al. 2006; Bria et al. 2001). This fulfills the needs of a variety of interested parties. It serves as a springboard for targeting areas where further research is required. It allows practitioners to better allocate resources. It allows policy makers to address deficiencies, or outright misconceptions, regarding biometrics. From an overarching societal perspective, this is key information as governments begin to rollout biometric-enabled identification documents (Sheng et al. 2006; Bria et al. 2001).

The use of scenario analysis within the realm of IT is relatively new. It has been used to study privacy concerns (Malhotra et al. 2004; Xu and Teo 2004), customer service (Resnick and Montania 2003), and ubiquitous commerce, or u-commerce (Sheng et al. 2006). As discussed by Webster and Trevino (1995, p. 1550), it has been used extensively in several other management areas including media choice (Straub and Karahanna 1998, marketing (Batsell and Lodish 1981), finance (Slovic 1972), personnel (Klaas and Wheeler 1990), organizational behaviour (Martocchio and Judge 1994), and strategic decision making (Hitt and Tyler 1991). According to Sheng et al. (2006, p. 15), the benefit of using scenarios is that it gives the researcher the ability to manipulate

conditions of variables, simulate user tasks, or represent a context for study (Xu and Teo 2004; Malhotra et al. 2004; Resnick and Montania 2003).

4.1.1 Experimental Manipulations

There are a variety of contexts (type of biometric, voluntariness versus involuntariness, biometric alone versus biometric and a PIN, single versus multiple biometrics, etc.) that are viable options to explore. However, in order to minimize the complexity it was decided to limit the investigation to two situational factors acting simultaneously. As previously discussed in Chapter 3 Section 3.2, Canadian bank personnel were involved in determining the two contextual variables to investigate.

Recall that control and voluntariness were the two factors (each with two levels) manipulated in the scenarios presented to subjects in this study. To review how these concepts were presented to respondents, the concept of the consumer having less control was operationalised as the bank maintaining a consumer's complete biometric; while more control was operationalised as the bank maintaining half the biometric identifier while the consumer retained half the biometric identifier on a smart card. Voluntariness was operationalised as the consumer having the option of using biometric identity authentication or a debit card, while involuntariness was operationalised as the bank using only biometric identity authentication for ATM use. The detailed wording of the scenarios is provided in Table 4-1 while Table 4-2 is a summary 2-by-2 matrix that provides the abbreviations that will subsequently be used to refer to the scenarios throughout the following discussion.

Table 4-1: Scenarios Used

Scenario 1 – Involuntary and Bank Control
For the following questions, imagine that you want to access your accounts at your bank's automatic teller machine (ATM). Your bank has discontinued debit cards with passwords and now **ONLY** uses biometric verification. Now your identity is verified through the use of your fingerprint (as biometric information). This fingerprint biometric information is stored at your bank. To access your bank accounts, you must place your index finger on a biometric scanner which instantaneously verifies a match of your fingerprint with the electronic version stored at the bank. Once a match is determined, you are given access to your bank accounts. **Note:** A biometric is a unique physical trait (such as fingerprints, facial characteristics, etc.) associated with an individual which could be used to authenticate the identity of that individual. The actual fingerprint is not stored by the bank. Rather, it is transformed into a unique mathematical expression that is used to verify your identity when your fingerprint is being scanned.

Scenario 2 – Involuntary and Shared Control

For the following questions, imagine that you want to access your accounts at your bank's automatic teller machine (ATM). Your bank has discontinued debit cards with passwords and now **ONLY** uses biometric verification. Now your identity is verified through the use of your fingerprint (as biometric information). However, only half of your biometric information is kept by your bank, while the other half resides on your bank card that you keep. Without the part of the biometric that is stored on your bank card, the part of the biometric stored by the bank is useless. To access your bank accounts, you must insert your bank card into the ATM and place your index finger on a biometric scanner. The biometric information stored on your bank card is combined with the biometric information stored at the bank to create a complete biometric record. Your scanned fingerprint is instantaneously compared to the complete biometric record obtained through your bank card and the bank. Once a match is determined, you are given access to your bank accounts.

Note: A biometric is a unique physical trait (such as fingerprints, facial characteristics, etc.) associated with an individual which could be used to authenticate the identity of that individual. The actual fingerprint is not stored by the bank. Rather, it is transformed into a unique mathematical expression that is used to verify your identity when your fingerprint is being scanned.

Scenario 3 – Voluntary and Bank Control

For the following questions, imagine that you want to access your accounts at your bank's automatic teller machine (ATM). Your bank has given you the **OPTION** of using biometric information instead of a debit card and password. Now your identity can be verified through the use of your fingerprint (as biometric information). This fingerprint biometric information is stored at your bank. If you opt into this service, you would place your index finger on a biometric scanner, which instantaneously verifies a match of your fingerprint with the electronic version stored at the bank. Once a match is determined, you would be given access to your bank accounts.

Note: A biometric is a unique physical trait (such as fingerprints, facial characteristics, etc.) associated with an individual which could be used to authenticate the identity of that individual. The actual fingerprint is not stored by the bank. Rather, it is transformed into a unique mathematical expression that is used to verify your identity when your fingerprint is being scanned.

Scenario 4 – Voluntary and Shared Control

For the following questions, imagine that you want to access your accounts at your bank's automatic teller machine (ATM). Your bank has given you the **OPTION** of using biometric information instead of a debit card and password. Now your identity can be verified through the use of your fingerprint (as biometric information). However, only half of your biometric information is kept by your bank, while the other half resides on your bank card that you keep. Without the part of the biometric that is stored on your bank card, the part of the biometric stored by the bank is useless. If you opt into this service, to access your bank accounts you would insert your bank card into the ATM and place your index finger on a biometric scanner. The biometric information stored on your bank card is combined with the biometric information stored at the bank to create a complete biometric record. Your scanned fingerprint is instantaneously compared to the complete biometric record obtained through your bank card and the bank. Once a match is determined, you are given access to your bank accounts.

Note: A biometric is a unique physical trait (such as fingerprints, facial characteristics, etc.) associated with an individual which could be used to authenticate the identity of that individual. The actual fingerprint is not stored by the bank. Rather, it is transformed into a unique mathematical expression that is used to verify your identity when your fingerprint is being scanned.

Table 4-2: Abbreviations of the Four Scenarios

Scenario 1 Involuntary and Bank Control (IBC)	Scenario 2 Involuntary and Shared Control (ISC)
Scenario 3 Voluntary and Bank Control (VBC)	Scenario 4 Voluntary and Shared Control (VSC)

In order to minimize potential bias as respondents moved from one scenario to the next while answering the same questions, a between subjects design was used in which respondents were given only one of the four scenarios (Keppel 1991). In addition, respondents were asked the questions regarding disposition to trust, risk, PIIT, and trust in one's bank prior to being given their scenario in order to establish the level of these traits

independently of the scenario thereby reducing any potential bias the latter might have on these pre-existing conditions. Also, the wording of each scenario was always at the top of the screen such that, if required, respondents could always refer to it while answering the survey questions.

4.2 Operationalisation of Constructs

The reflective constructs used were adapted from instruments developed and validated in prior studies. The trust scale is adapted from Gefen et al. (2003a) which is consistent with other studies that treat the three trust belief characteristics of benevolence, integrity, and competence as a single construct (Gefen et al. 2005; Gefen 2004; Pavlou and Gefen 2004; Doney and Cannon 1997). Table 4-3 shows the wording of the construct items and their sources.

Table 4-3: Sources for Reflective Construct Items

Question
PIIT [Source: Agarwal and Prasad (1998)]
PIIT1: If I heard about a new technology, I would look for ways to experiment with it.
PIIT2: Among my peers, I am usually the first to try out new technologies.
PIIT3: In general, I am hesitant to try out new technologies.
PIIT4: I like to experiment with new technologies.
Disposition to Trust [Source: Cheung and Lee (2001)]
DT1: It is easy for me to trust a person/thing.
DT2: My tendency to trust a person/thing is high.
DT3: I tend to trust a person/thing, even though I have little knowledge of it.
DT4: Trusting someone or something is not difficult.
Risk Propensity [Source: Jackson Personality Inventory as cited in Baldwin et al. (2005)]
Risk1: I enjoy taking risks.
Risk2: I do not avoid situations that have uncertain outcomes.
Risk3: Taking risks does not bother me if the gains involved are high.
Risk4: I consider security an important element in every aspect of life.
Risk5: People have told me I seem to enjoy taking chances.
Risk6: I often take risks even when there is another alternative.
Trust [Source: Gefen et al. (2003a)]
Trust1: Based on my experience with my bank in the past, I know it is honest.
Trust2: Based on my experience with my bank in the past, I know it cares about its customers.
Trust3: Based on my experience with my bank in the past, I know it is not opportunistic.
Trust4: Based on my experience with my bank in the past, I know it is predictable.
Trust5: Based on my experience with my bank in the past, I know it knows its market.

Perceived Usefulness [Source: Moore and Benbasat (1991)]
Usefulness1: When faced with this scenario, I would be able to accomplish my banking more quickly.
Usefulness 2: When faced with this scenario, I would be able to accomplish my banking more easily.
Usefulness 3: When faced with this scenario, I would find using biometrics enhances my effectiveness.
Usefulness 4: When faced with this scenario, I would find biometrics useful.
Attitude [Source: Morris and Venkatesh (2000)]
Attitude1: When faced with this scenario, using biometrics for identity verification is a good idea.
Attitude 2: When faced with this scenario, using biometrics for identity verification is a wise idea.
Attitude 3: When faced with this scenario, I like the idea of using biometrics for identity verification.
Attitude 4: When faced with this scenario, using biometrics for identity verification would be pleasant.

Recall from Section 3.3.1 above that five concerns with respect to biometrics were identified: security, privacy, function creep, physical harm, and inconvenience. Previous research [see Pavlou et al. (2007)] suggests that function creep is a privacy issue given its definition as the expansion of the use of information beyond its intended application to include systems not agreed to by the owners of the information. Therefore, the items for the privacy and security concerns construct (see Table 4-4) were adapted from items previously validated by Pavlou et al. (2007).

Table 4-4: Privacy and Security Concerns [Source: Pavlou et al. (2007)]

Question
PSC1: When faced with this scenario, I am concerned that my bank is collecting too much information about me.
PSC2: When faced with this scenario, it bothers me that my bank asks me for my biometric information.
PSC3: When faced with this scenario, I am concerned about my privacy.
PSC4: When faced with this scenario, I have doubts as to how well my privacy is protected.
PSC5: When faced with this scenario, I am concerned that my biometric information could be misused.
PSC6: When faced with this scenario, I am concerned that my biometric information could be accessed by unknown parties.
PSC7: When faced with this scenario, I would feel secure providing biometric information to my bank.

PSC8: When faced with this scenario, the potential security issues of sharing my biometric information with my bank would be a major obstacle to my using this form of identity verification.
PSC9: When faced with this scenario, I believe that, overall, banks are a safe place to keep biometric information.
PSC10: When faced with this scenario, I would feel totally safe providing biometric information to my bank.

4.3 Open-Ended Questions

Four open-ended questions were included at the end of the survey to provide respondents the opportunity to give any additional information that might not have been captured in the survey as well as to provide further interpretation and insight with respect to the quantitative results. As with the survey questions, the scenarios were always visible at the top of the page such that respondents could refer back to the details in answering these questions. The questions were:

- In the above scenario, what do you feel are the benefits/advantages of using biometrics?
- In the above scenario, what concerns do you have using biometrics?
- Please provide any other comments regarding the use of biometrics.
- Finally, have you ever been a victim of identity theft. If yes, please explain.

4.4 Structural Equation Modeling

Structural Equation Modeling (SEM) allows the investigation and analysis of unobservable (latent) variables (constructs) "that are indirectly inferred from multiple observed measures (alternatively termed as indicators or manifest variables)." (Chin 1998, p. vii) While this method has been employed by the social sciences for some time (Anderson and Gerbing 1988), it has also been embraced by business academics doing research in marketing (Hsu et al. 2006; Fornell and Bookstein 1982; Fornell and Larcker 1981a; Fornell and Larcker 1981b) and strategic management (Hulland 1999). It is also being used with increasing frequency within in the field of information systems (Gefen et al 2000; Chin 1998).

SEM is a "multivariate technique combining aspects of multiple regression (examining dependence relationships) and factor analysis (representing unmeasured concepts with multiple variables) to estimate a series of interrelated dependence relationships simultaneously" (Gefen et al. 2000, p. 72). There are two SEM methods available to researchers, covariance-based (such as LISREL and AMOS) and component-based PLS. For this research, the latter method is employed. There are multiple reasons for this choice.

First, covariance-based methods are preferred when the research is more confirmatory in nature (i.e. the theory is more established and goal of the study is further testing and development); PLS, on the other hand, is more applicable to exploratory

research (i.e. testing models/theories in the early stages of development) (Chin et al. 2003; Gefen et al. 2000; Anderson and Gerbing 1988). Therefore, as there is a lack of research within the realm of consumer acceptance of biometrics, PLS seems more appropriate. Second, prediction accuracy is greater for PLS than for covariance-based methods (Anderson and Gerbing 1988). Third, PLS can be applied to a small sample size relative to covariance-based methods (Gefen et al. 2000; Fornell and Bookstein 1982). Chin et al. (2003) and Gefen et al. (2000) give a standard rule of thumb that sample size for PLS should be the larger of: (1) 10 times the number of items for the most complex construct; and (2) 10 times the largest number of independent variables impacting a dependant variable. In the model presented above, the most complex construct has 10 items and the largest number of independent variables affecting a dependant variable is 7. Thus, the minimum sample size required is 100 respondents. Finally, PLS more easily supports the combined use of formative and reflective constructs, which is the case for the proposed model.

It should be noted that PLS will be run on the entire sample to investigate the validity of the model as a whole. Post hoc analysis will then be performed via ANOVA testing to further explore what differences, if any, exist among the scenarios.

4.5 Sample

The sample was collected from MBA students at two major Canadian universities and included both full-time and part-time students. To participate in the study, subjects had to 1) be over 18; 2) not work for a bank; 3) have a bank account; 4) live in Canada; and 5) use an ATM. While there are some shortcomings to using MBA students, it is preferable to using undergraduate students since, according to Remus (1989), "professional or graduate students...typically make better decisions than undergraduate students" (Hassanein and Head 2007, p. 695). In addition, when compared to undergraduate students, they will have more varied experiences, income levels, and educational backgrounds as well as provide for a greater variation in age; this argument is supported by the fact that the MBA students were both full-time and part-time.

Participants were contacted either via e-mail or by visiting their classroom and asking for volunteers, and were randomly assigned to one of the four scenarios. In both methods of contact, respondents were directed to a website to fill in the survey. The online survey package used was LimeSurvey™. For those approached in class, they were given a consent form to sign and asked to provide their e-mail address so that the URL could be sent to them. For those approached via e-mail, they provided consent by clicking on the "I Agree" button prior to taking the survey. To preserve anonymity, the e-mails were sent out as blind carbon copies such that e-mail addresses could not be viewed by other participants and also to ensure no record of e-mail addresses was maintained in the researcher's "sent" mailbox/folder.

No direct compensation was received by the students approached solely via e-mail while those approached directly by visiting their classroom were given $5 in gift

certificates to Tim Horton's, which is a popular Canadian coffee shop chain, in exchange for their signed consent and e-mail address in the good faith understanding that they would fill out the survey upon receipt of the URL via e-mail. While ultimately this action did not result in 100% response from those that did receive the incentive, the response was greater when compared to those students contacted by e-mail alone. In addition, all respondents that provided their e-mail address were included in a draw for a $100 gift certificate to Chapters or Titles (the McMaster University Bookstore).

Chapter 5 Data Analysis and Results

5.1 Survey Administration

The survey was administered in two waves. The first wave occurred in August 2008 and targeted full-time, co-op, and part-time MBA students at one of the universities. The second wave occurred from September through October 2008 and targeted full-time and part-time students entering the MBA program at the same university as above, and all full-time and part-time students at the second university. Of the 521 potential respondents solicited via e-mail, 100 usable surveys were obtained for a response rate of 19.2%. Classroom solicitation resulted in 245 volunteers which generated 175 usable surveys for a response rate of 71.4%. The total number of usable surveys was 275 which is an overall response rate of 35.9%.

5.2 Participant Demographics and Scenario Coverage

Aside from standard demographic questions such as gender and age, several additional questions were asked based upon discussions with the bank. Table 5-1 summarizes the participant demographics while Table 5-2 gives the breakdown of the respondents in terms of the two contextual variables (control and voluntariness) and the scenarios that provide the contexts.

Table 5-1: Demographics

Demographic	Categories	Frequency	Percentage
Gender	Female	115	41.8%
	Male	160	58.2%
Age	18-24	65	23.7%
	25-34	159	57.8%
	35-44	43	15.6%
	45-54	8	2.9%
Income	< $25k	53	19.3%
	$25k to $50k	45	16.4%
	$50k to $75k	81	29.4%
	$75k to $100k	45	16.4%
	> 100k	24	8.7%
	No Answer	27	9.8%
Education	Some Post Secondary	2	0.7%
	Comp Post Secondary	159	57.8%
	Graduate Degree	114	41.5%

ATM Use	< Once per Month	21	7.6%
	Once per Month	56	20.4%
	Once per Week	152	55.3%
	> Once per Week	46	16.7%

As previously mentioned, since the context being investigated is ATM use, those respondents that do not use ATMs were removed from the survey. In addition, as frequency of ATM use may be an influencing factor in people's attitudes towards biometrics, respondents were asked how often they used ATMs.

Table 5-2: Context and Scenario Coverage

Context	Categories	Frequency	Percentage
Control	Bank	149	54.2%
	Shared	126	45.8%
Voluntariness	Involuntary	136	49.5%
	Voluntary	139	50.5%
Scenario	Inv and Bank Control	77	28.0%
	Inv and Shared Control	59	21.4%
	Vol and Bank Control	72	26.2%
	Vol and Shared Control	67	24.4%

In addition to the looking at the interplay between control and voluntariness via the scenarios, this research also wanted to look at the effects of these two contexts individually. Although the distribution between bank control and shared control slightly favoured bank control, the distribution between involuntary and voluntary was almost equal.

5.3 Evaluation of Reflective Constructs

Various tests were conducted to assess the validity of the items and their corresponding constructs. Content validity is defined as the extent to which the items portray a representative and comprehensive measurement of the constructs used in the proposed model. Content validity is assessed based upon the process employed to generate the items. Cronbach (1971) and Kerlinger (1964) suggest that content validity is supported by generating items from a universal pool. While slight modifications were necessary to make the items more applicable to the subject matter under investigation, the items used in this study were developed and validated in prior research. Therefore, the content validity requirement has been satisfied.

Convergent validity was assessed using a principal components analysis with varimax rotation as shown in Table 5-3.

Table 5-3: Initial Convergent Validity Assessment – Principal Components with Varimax Rotation

	1	2	3	4	5	6
PITT 1	**.830**	.006	.035	.022	.093	.126
PITT 2	**.818**	.123	.146	-.065	-.003	.073
PITT 3	**.734**	-.002	.189	.051	-.075	.143
PITT 4	**.879**	.038	.135	.052	.069	.087
DT 1	.095	**.894**	.120	.049	.046	.099
DT 2	.044	**.901**	.136	.116	.046	.066
DT 3	.020	**.882**	.092	.096	-.002	.063
DT 4	-.011	**.818**	.178	.175	-.062	.075
Risk 1	.134	.175	**.836**	.029	-.046	.011
Risk 2	-.005	.123	**.728**	.006	-.086	.168
Risk 3	.212	.124	**.741**	-.023	.064	.117
Risk 4	-.239	.151	**.091**	-.001	-.227	.309
Risk 5	.074	.066	**.857**	.006	.062	.009
Risk 6	.104	.048	**.784**	.049	.122	.051
Trust 1	-.008	.086	.083	**.767**	.036	.118
Trust 2	-.057	.052	-.062	**.854**	.021	.148
Trust 3	-.035	.065	-.007	**.768**	.104	.044
Trust 4	.088	.140	.102	**.613**	-.022	.107
Trust 5	.056	.045	-.056	**.731**	-.030	.038
Useful 1	.005	.020	.046	.021	**.823**	.480
Useful 2	.032	.037	.058	.037	**.813**	.503
Useful 3	.084	.005	.099	.089	**.715**	.593
Useful 4	.030	.011	.096	.135	**.367**	.794
Att 1	.070	.047	.055	.076	.088	**.919**
Att 2	.069	.048	.048	.067	.050	**.921**
Att 3	.037	.058	.109	.111	.103	**.910**
Att 4	.088	.163	-.017	.074	.276	**.820**

With the cutoff eigenvalue set to one, this yielded six factors. Hair et al. (1995) suggested that an item is significant if its factor loading is greater than 0.50. Using this threshold, two items were dropped. Risk 4 was dropped as it didn't meet the threshold. Usefulness 4 was also dropped due to not meeting the threshold; in addition, it had high cross-loadings with another construct. After the removal of these two items, the principal components analysis with varimax rotation was re-run. The net results of the convergent validity assessment are shown in Table 5-4.

When removing items based upon principal components analysis, it is also useful to examine the face validity of these items to understand why they did not meet the suggested threshold and load to the same degree as the other items. Risk 4 stated "I consider security an important element in every aspect of life". Perhaps in the minds of the respondents, this was too all encompassing as it potentially suggests that the respondent will do nothing without first considering the aspect of security. Furthermore, such a statement could suggest a heightened level of paranoia that most respondents do not possess, hence the low loading. Turning to Usefulness 4, this item states "When faced with this scenario, I would find biometrics useful". Given the word "useful" in the item, this creates a bit of a conundrum. However, perhaps it suffers from a problem similar to that as the Risk 4 item. In other words, the other usefulness items focus on doing banking "more quickly", "more easily", and enhancing effectiveness which imply specific reasons for the usefulness of biometrics whereas the term "useful" on its own may be interpreted as either too all encompassing and/or too vague. In addition, it should be noted that Usefulness 4 crossloads on Attitude, and to a such a degree that it actually passes the suggested threshold. This may suggest that, in the minds of the respondents, the wording of the item has an element of the attitude construct. Finally, based upon other research [see Zhang et al. (2006) and Petter et al. (2007)] and as suggested later (see Section 6.6 Future Research) perhaps the original usefulness construct as envisioned by Davis (1989) is too broad for examining acceptance of present-day technologies and/or contexts of use and should be broken down into more refined constructs, such as convenience (Zhang et al. 2006), or treated as a combined reflective and formative construct (Petter et al. 2007).

Table 5-4: Convergent Validity Assessment – Re-Run Principal Components with Varimax Rotation

Item	PIIT	Disposition to Trust	Risk	Trust	Usefulness	Attitude
PIIT 1	**.836**	.005	.032	.024	.116	.070
PIIT 2	**.832**	.118	.138	-.061	.037	.019
PIIT 3	**.742**	-.004	.186	.053	-.057	.139
PIIT 4	**.884**	.035	.130	.052	.071	.052
DT 1	.099	**.896**	.120	.047	.061	.074
DT 2	.045	**.902**	.136	.114	.065	.038
DT 3	.022	**.884**	.092	.094	.012	.048
DT 4	-.005	**.818**	.178	.172	-.059	.093
Risk 1	.140	.175	**.835**	.026	-.052	.016
Risk 2	.001	.125	**.732**	.007	-.066	.186
Risk 3	.220	.123	**.741**	-.023	.079	.093
Risk 5	.076	.070	**.857**	.005	.075	-.038
Risk 6	.107	.051	**.784**	.050	.152	-.008
Trust 1	-.001	.089	.085	**.771**	.079	.067
Trust 2	-.051	.056	-.059	**.858**	.053	.117
Trust 3	-.026	.067	-.008	**.770**	.118	-.013
Trust 4	.083	.136	.107	**.609**	-.065	.178
Trust 5	.060	.049	-.055	**.733**	-.014	.002
Useful 1	.026	.017	.047	.033	**.900**	.317
Useful 2	.055	.034	.058	.050	**.895**	.341
Useful 3	.109	.008	.101	.104	**.829**	.407
Att 1	.094	.051	.068	.096	.248	**.912**
Att 2	.091	.052	.062	.086	.211	**.929**
Att 3	.059	.064	.123	.131	.272	**.882**
Att 4	.114	.164	-.008	.094	.440	**.753**

Table 5-5 shows the values for Cronbach's alpha, composite reliability, and average variance extracted (AVE) for the six reflective constructs used. Nunnally (1978) recommends that the Cronbach's α of a scale should be greater than 0.70 for items to be used together as a construct. Since the values range from 0.816 for trust to 0.956 for usefulness, the test for construct reliability has been satisfied. Composite reliability is a measure of internal consistency for each construct and should have a value greater than

0.70 according to Fornell and Larcker (1981). The composite reliability scores (from 0.872 for trust to 0.971 for usefulness) are all above the suggested threshold.

Table 5-5: Cronbach's α, Composite Reliability and AVE

	PIIT	Disposition to Trust	Risk	Trust	Attitude	Usefulness
α-value	0.860	0.918	0.867	0.816	0.954	0.956
Comp Rel	0.904	0.941	0.903	0.872	0.967	0.971
AVE	0.703	0.800	0.651	0.578	0.879	0.919

Discriminant validity is established if the square root of the AVE for each construct is greater than the threshold of 0.50 as suggested by Fornell and Larcker (1981) and, according to Chin (1998), is also considerably greater than the correlation of the specific construct with any of the other constructs in the model. Table 5-6 shows the correlation matrix of the six constructs with the square root of the AVE in bold along the diagonal. Given that the square roots of the AVEs are both above 0.50 and are much larger than the correlations to other constructs, discriminant validity has been demonstrated. In fact, following the suggestion of a more stringent approach, proposed by Gefen et al. (2000), of using the AVEs themselves instead of their square roots across the diagonal renders the same conclusion with respect to discriminant validity.

Table 5-6: Correlation Matrix with Square-Roots of AVE

	PIIT	Disposition to Trust	Risk	Trust	Attitude	Usefulness
PIIT	**0.838**					
Disposition to Trust	0.117	**0.894**				
Risk	0.307	0.292	**0.807**			
Trust	0.053	0.237	0.061	**0.760**		
Attitude	0.202	0.186	0.168	0.223	**0.938**	
Usefulness	0.154	0.084	0.156	0.153	0.640	**0.959**

5.4 Common Methods Bias

Due to the method of data collection, common method bias may be an issue and needs to be assessed. Common method bias, or variance, occurs when both the independent and dependent variables are collected at the same time and from the same source (Liang et al. 2007, Podsakoff et al. 2003). This is of particular concern "when respondents are asked to fill out items that tap into independent and dependent variables within the same survey instrument. Overall, method variance affects the assessment of a particular trait or behaviour, especially when self-reports are used" (Serenko 2005, p. 73).

In order to assess common method bias, Harman's one-factor test (Podsakoff and Organ 1986, Harman 1967) was conducted. An exploratory factor analysis was run on all the items using the unrotated solution to a principal components analysis. The solution generated six factors with an eigenvalue greater than one. The first factor accounted for 25.7% of the variance. Since the variables do not load on a single general factor, this test indicates that common method bias is not substantial and is therefore not likely contaminating the results.

In addition, "following Podsakoff et al. (2003) and Williams et al. (2003), [a common method factor] was included in the PLS model...whose indicators included all the principal constructs' indicators and calculated each indicator's variances substantively explained by the principal construct and by the method" (Liang et al. 2007). The results are presented in Table 5-7.

Table 5-7: Common Methods Bias Analysis

	Construct	Indicator	Loading	Sig.	(Loading)²
Common Method Factor Loadings (R2)	Attitude	Att 1	-0.050		0.003
		Att 2	-0.087	*	0.008
		Att 3	0.023		0.001
		Att 4	0.121	*	0.015
	Control	Control 1	0.154	*	0.024
	Disposition to Trust	DT 1	0.029		0.001
		DT 1	0.006		0.000
		DT 3	-0.043		0.002
		DT 4	0.008		0.000
	PIIT	PIIT 1	-0.008		0.000
		PIIT 2	-0.023		0.001
		PIIT 3	0.026		0.001
		PIIT 4	0.007		0.000
	Risk	Risk 1	-0.045		0.002
		Risk 2	0.025		0.001
		Risk 3	0.092		0.008
		Risk 5	-0.087	*	0.008
		Risk 6	0.016		0.000
	Trust	Trust 1	0.052		0.003
		Trust 2	-0.035		0.001
		Trust 3	-0.041		0.002
		Trust 4	0.127		0.016
		Trust 5	-0.088		0.008
	Usefulness	Use 1	-0.145	***	0.021
		Use 2	-0.090	**	0.008
		Use 3	0.028		0.001
	Voluntariness	Vol 1	-0.001		0.000
	Average		**-0.001**		**0.005**

	Construct	Indicator	Loading	Sig.	(Loading)²
Substantive Constructs Factor Loadings (R2)	Attitude	Att 1	0.997	***	0.994
		Att 2	1.000	***	1.000
		Att 3	0.928	***	0.861
		Att 4	0.791	***	0.626
	Control	Control 1	1.000	***	1.000
	Disposition to Trust	DT 1	0.896	***	0.803
		DT 1	0.921	***	0.848
		DT 3	0.916	***	0.839
		DT 4	0.849	***	0.721
	PIIT	PIIT 1	0.839	***	0.704
		PIIT 2	0.856	***	0.733
		PIIT 3	0.764	***	0.584
		PIIT 4	0.896	***	0.803
	Risk	Risk 1	0.883	***	0.780
		Risk 2	0.729	***	0.531
		Risk 3	0.740	***	0.548
		Risk 5	0.904	***	0.817
		Risk 6	0.784	***	0.615
	Trust	Trust 1	0.762	***	0.581
		Trust 2	0.877	***	0.769
		Trust 3	0.788	***	0.621
		Trust 4	0.596	***	0.355
		Trust 5	0.761	***	0.579
	Usefulness	Use 1	1.000	***	1.000
		Use 2	1.000	***	1.000
		Use 3	0.928	***	0.861
	Voluntariness	Vol 1	1.000	***	1.000
	Average		**0.867**		**0.762**

Significance levels: *** 0.001, ** 0.01, * 0.05

The average of the substantively explained variance of the indicators was 0.762, while the average method variance is 0.005, resulting in a ratio of substantive variance to method variance of approximately 152:1. In addition, the majority of the factor loadings were not significant. Based upon the results of these two tests, it was concluded that common method variance is unlikely to be a serious concern for this study.

5.5 Evaluation of Formative Construct

Recall that the direction of causality in reflective items is from the construct to the items, whereas in formative constructs the direction of causality is from the items to the construct. Also, recall that, while there might be some interplay amongst the items, a change in one item does not imply or necessitate a change in the other; and, finally a change in the construct does entail a change in all the causal measures. This has implications with respect to the evaluation of formative constructs. Given the composite nature of formative constructs, the underlying items do not need to correlate and are presumed not to covary. In fact, formative constructs must be examined for multicollinearity since, if the items are too highly correlated, they are essentially measuring the same thing (Bollen 1989). As such, reflective construct validation methods, such as common factor analysis, AVEs, and Cronbach's alpha, are not applicable to the evaluation of formative constructs (Petter et al. 2006).

The method to examine the validity of the formative construct perceived privacy and security concerns will be that prescribed by Diamantopoulos and Winklhofer (2001). The measurement items used will be examined for multicollinearity and external validity using linear regression and PLS with a two construct Multiple Indicators, Multiple Causes (MIMIC) model (Jarvis et al. 2003; Diamantopoulos and Winklhofer 2001).

A linear regression was run using the indicators for perceived privacy and security as the independent variables and the mean of the attitude items as the dependent variable. Table 5-8 shows the initial correlation matrix and VIFs (variance inflation factors). A VIF of 10 is indicative of problems due to multicollinearity in traditional statistics theory; however, since multicollinearity poses more of a concern in formative measures, a more stringent cutoff should be applied (Petter et al. 2006). The cutoff suggested by Diamantopoulos and Siguaw (2006) is 3.3. Using this method iteratively, the resultant correlation matrix and VIFs are shown in Table 5-9. Aside from being below the prescribed VIF value of 3.3, the highest correlation between items is 0.728, which is below the 0.8 limit suggested by Stevens (1996).

As previously suggested, when removing items from reflective constructs, it is worthwhile to examine the face validity of the dropped item to see if its removal makes logical sense. This is also true in the case of formative constructs and perhaps even more important as the items, by definition, are not measuring exactly the same thing and, as such, the removal of an item may not be logically justifiable since it may be addressing an element of the construct that is not being explored by the other items. Upon reviewing the items that were dropped, there did not appear to be any area that was not being addressed by the retained items. In other words, the remaining items appear to be measuring similar dimensions as the dropped items such that the construct has retained all the logical elements it is trying to measure.

Table 5-8: Privacy and Security Concerns – Attitude, Initial Correlation Matrix and VIFs

	Attitude	PSC1	PSC2	PSC3	PSC4	PSC5	PSC6	PSC7	PSC8	PSC9	PSC10	VIF
Attitude	1.000	-.596	-.622	-.545	-.496	-.521	-.470	-.616	-.618	-.600	-.676	
PSC1		1.000	.883	.818	.728	.698	.546	.617	.712	.644	.676	5.321
PSC2			1.000	.819	.749	.704	.558	.655	.741	.651	.688	5.771
PSC3				1.000	.831	.749	.629	.614	.739	.636	.672	5.145
PSC4					1.000	.763	.700	.615	.720	.613	.698	4.273
PSC5						1.000	.779	.617	.721	.613	.683	3.970
PSC6							1.000	.532	.682	.579	.623	3.039
PSC7								1.000	.654	.622	.684	2.251
PSC8									1.000	.693	.733	3.487
PSC9										1.000	.772	2.844
PSC10											1.000	3.598

Table 5-9: Privacy and Security Concerns – Attitude, Terminal Correlation Matrix and VIFs

	Attitude	PSC1	PSC4	PSC6	PSC7	PSC8	PSC9	VIF
Attitude	1.000	-.596	-.496	-.470	-.616	-.618	-.600	
PSC1		1.000	.728	.546	.617	.712	.644	2.741
PSC4			1.000	.700	.615	.720	.613	3.139
PSC6				1.000	.532	.682	.579	2.315
PSC7					1.000	.654	.622	2.071
PSC8						1.000	.693	3.237
PSC9							1.000	2.299

A two construct MIMIC test was constructed in PLS using perceived privacy and security concerns as the exogenous variable and attitude as the endogenous variable. This test is particularly important when indicators have been eliminated from the original construct (Diamantopoulos and Winklhofer 2001) as is the case here. The path between the two constructs should be greater than zero and significant. Table 5-10 shows that both of these requirements have been satisfied.

Table 5-10: Privacy and Security Concerns – Attitude, MIMIC Model

Path Beta	t-statistic	Significance Level	R-Squared
-0.711	20.668	0.000	0.506

A summary of the indices for the formative constructs and the indicators for the reflective constructs are provided in Table 5-11 and Table 5-12 respectively.

Table 5-11: Descriptive Statistics and Indices for Formative Constructs

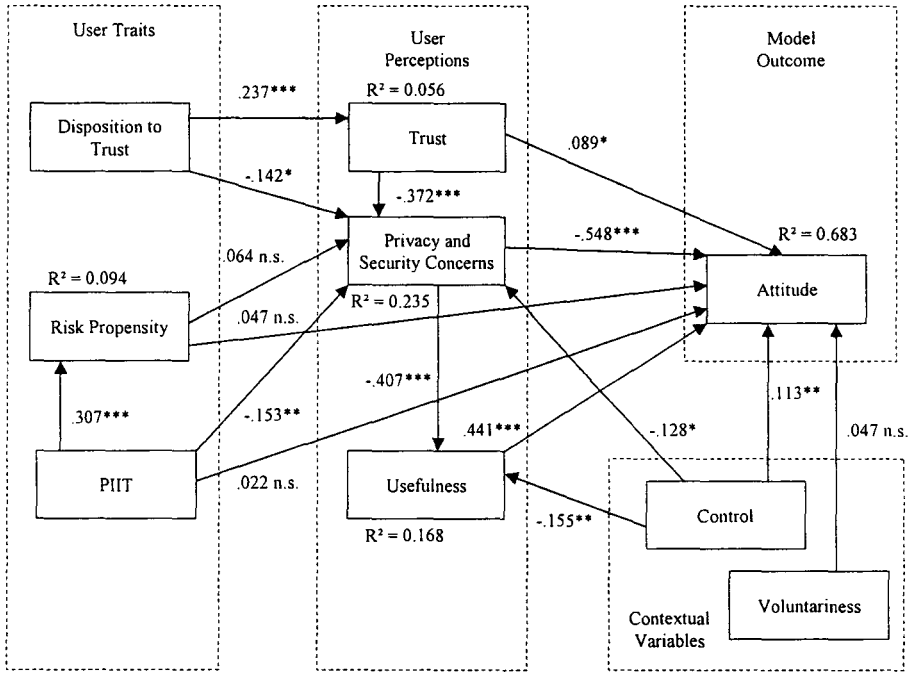
Construct	Item	Mean	Std. Dev.	Weight	t-stat	Sig Level
Privacy and Security Concerns	PSC1	3.93	1.770	0.260	2.473	0.014
	PSC4	4.55	1.844	0.092	0.786	0.433
	PSC6	4.95	1.579	0.037	0.361	0.718
	PSC7	4.05	1.657	0.438	5.128	0.000
	PSC8	4.03	1.747	0.157	1.200	0.231
	PSC9	3.86	1.516	0.409	3.799	0.000

Table 5-12: Descriptive Statistics and Indicators for Reflective Constructs

Construct	Item	Mean	Std. Dev.	Loading	t-stat	Sig Level
PIIT	PIIT1	5.11	1.215	0.808	22.791	0.000
	PIIT2	4.21	1.565	0.830	27.880	0.000
	PIIT3	5.09	1.403	0.818	20.220	0.000
	PIIT4	5.08	1.325	0.895	46.547	0.000
Disposition to Trust	DT1	4.20	1.516	0.894	38.823	0.000
	DT2	4.09	1.551	0.913	40.865	0.000
	DT3	3.46	1.512	0.892	47.472	0.000
	DT4	3.98	1.505	0.879	33.563	0.000
Risk	Risk1	4.63	1.335	0.851	34.037	0.000
	Risk2	4.65	1.271	0.740	12.802	0.000
	Risk3	4.96	1.192	0.837	30.753	0.000
	Risk5	4.18	1.371	0.827	20.167	0.000
	Risk6	3.71	1.378	0.774	18.373	0.000
Trust	Trust1	4.97	1.270	0.798	22.801	0.000
	Trust2	4.49	1.410	0.859	35.953	0.000
	Trust3	3.80	1.378	0.762	20.547	0.000
	Trust4	4.71	1.197	0.666	12.089	0.000
	Trust5	4.82	1.216	0.702	14.197	0.000
Attitude	Att1	4.47	1.564	0.956	144.018	0.000
	Att2	4.32	1.557	0.956	133.748	0.000
	Att3	4.29	1.662	0.946	85.418	0.000
	Att4	4.07	1.476	0.891	55.423	0.000
Usefulness	PU1	3.88	1.615	0.958	141.947	0.000
	PU2	3.83	1.597	0.970	177.055	0.000
	PU3	3.73	1.607	0.947	123.911	0.000

5.6 Evaluation of Structural Model

The preceding section established the validity of the measurement instrument used in data collection. This section will assess the validity of the structural model and the associated hypotheses.



Significance levels: *** 0.001, ** 0.01, * 0.05, n.s. not significant

Figure 5-1: Proposed Research Model SmartPLS Results

The structural model was evaluated using SmartPLS (v. 2.0.M3) and is depicted in Figure 5-1. The model was tested by using bootstrapping. This is one of several non-parametric techniques available to estimate the significance of the path coefficients (Tenenhaus et al. 2005; Chin 1998). Two other methods are blindfolding and jackknifing. Blindfolding procedures can lead to very small standard deviations which can in turn lead to systematically significant parameters; and jackknifing can lead to a potential loss of robustness (Tenenhaus et al. 2005). In addition, jackknifing is considered to be an estimation of bootstrapping (Efron and Tibshirani 1993). Bootstrapping draws N resamples to obtain N sets of parameter estimates (Chin 1998) with each resample containing the same number of cases as the original sample (Tenenhaus et al. 2005; Andrews and Buchinsky 2000; Efron 2000). In this research, 500 resamples were used "as a higher number may lead to more reasonable standard error estimates" (Tenehaus et al. 2005, p. 176). The hypotheses, paths, path coefficients, etc. are detailed in Table 5-13.

Table 5-13: Summary of Findings of Support for Hypotheses

Hypothesis	Path	Beta	Standard Error	t-statistic	p-value	Validation
H1	Usefulness -> Attitude	0.441	0.045	9.764	< 0.001	Supported
H2	PSC -> Attitude	-0.548	0.043	12.914	< 0.001	Supported
H3	PSC -> Usefulness	-0.407	0.055	7.470	< 0.001	Supported
H4	Trust -> Attitude	0.089	0.043	2.054	< 0.05	Supported
H5	DT -> Trust	0.237	0.053	4.447	< 0.001	Supported
H6	Risk -> PSC	0.064	0.066	0.980	0.328	Rejected
H7	Trust -> PSC	-0.372	0.062	6.055	< 0.001	Supported
H8	DT -> PSC	-0.142	0.058	2.445	< 0.05	Supported
H9	Risk -> Attitude	0.047	0.041	1.144	0.254	Rejected
H10	PIIT -> Risk	0.307	0.052	5.852	< 0.001	Supported
H11	PIIT -> Attitude	0.022	0.039	0.571	0.568	Rejected
H12	PIIT -> PSC	-0.153	0.058	2.629	< 0.01	Supported
H13	Control -> Attitude	0.113	0.035	3.280	< 0.01	Supported
H14	Control -> PSC	-0.128	0.055	2.343	< 0.05	Supported
H15	Control -> Usefulness	-0.155	0.053	2.909	< 0.01	Supported
H16	Voluntariness -> Attitude	0.047	0.036	1.306	0.193	Rejected

5.7 Simplified Model

Although the hypothesized relationships were developed based upon an examination of the extant literature, not all the paths were significant. Most notably, it is the paths from the innate traits that are non-significant. As such, following Kaplan's (2000) recommendation, in which the theoretically developed research model is modified and re-run, a simplified model was developed in which the non-significant paths were removed, the context of voluntariness was eliminated, and the risk propensity construct was dropped. Voluntariness was removed as its one hypothesized path was not significant. Risk propensity was dropped due to the fact that, while the path from PIIT to

risk propensity was significant, the two paths emanating from risk propensity to privacy and security concerns and attitude were not significant.

The simplified model was re-tested with respect to Cronbach's alpha, composite reliability, and the square-roots of the AVEs versus the correlations between reflective constructs. The results are shown in Table 5-14. With some extremely small changes to the values associated with PIIT, the figures were virtually unchanged after the adjustments were made.

Table 5-14: Cronbach's α, Composite Reliability, AVE, and Square-Root of AVE

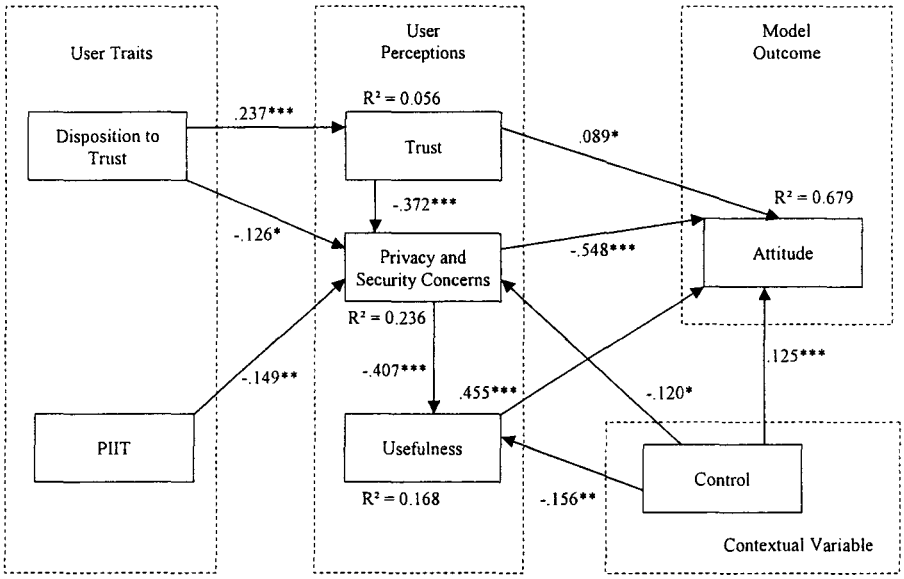
	PIIT	Disposition to Trust	Trust	Attitude	Usefulness
PIIT	**0.831**				
DispTrust	0.108	**0.894**			
Trust	0.062	0.237	**0.760**		
Attitude	0.207	0.186	0.223	**0.938**	
Usefulness	0.153	0.084	0.153	0.640	**0.959**
α-value	0.860	0.918	0.816	0.954	0.956
Comp Rel	0.899	0.941	0.872	0.967	0.971
AVE	0.690	0.800	0.578	0.879	0.919

The simplified structural model was again evaluated using SmartPLS and bootstrapping with 500 resamples. The results are shown in Figure 5-2 and Table 5-15. Comparing Figure 5-2 with Figure 5-1, one can see that the overall predictive power of the simplified model ($R^2 = 0.679$) is virtually unchanged from the original model ($R^2 = 0.683$) and that the same can be said for the R-squared values for trust, privacy and security concerns, and usefulness. Looking at Table 5-15, one can also see that all the remaining paths are significant. The simplified model will be used for the purpose of exploring effect sizes.

Table 5-15: Summary of Findings of Support for Hypotheses

Hypothesis	Path	Beta	t-statistic	p-value	Signif	Validation
H1	Usefulness -> Attitude	0.455	10.509	< 0.001	***	Supported
H2	PSC -> Attitude	-0.548	12.741	< 0.001	***	Supported
H3	PSC -> Usefulness	-0.407	7.345	< 0.001	***	Supported
H4	Trust -> Attitude	0.089	2.118	< 0.05	*	Supported
H5	DT -> Trust	0.237	4.124	< 0.001	***	Supported
H7	Trust -> PSC	-0.372	5.844	< 0.001	***	Supported
H8	DT -> PSC	-0.126	2.136	< 0.05	*	Supported
H12	PIIT -> PSC	-0.149	2.760	< 0.01	**	Supported
H13	Control -> Attitude	0.125	3.977	< 0.001	***	Supported
H14	Control -> PSC	-0.120	2.125	< 0.05	*	Supported
H15	Control -> Usefulness	-0.156	2.957	< 0.01	**	Supported

Significance levels: *** 0.001, ** 0.01, * 0.05, n.s. not significant



Significance levels: *** 0.001, ** 0.01, * 0.05, n.s. not significant

Figure 5-2: Proposed Simplified Model SmartPLS Results

5.8 Effect Sizes

The impact of individual constructs can be examined to assess the predictive power and quality of a model. The calculation of effect size (f^2) allows us to determine the contributions of independent variables upon the R-squared of dependent variables (Chin 1998). Using Chin's (1998) formula and Cohen's (1988) guidelines with respect to effect sizes – 0.02 (small), 0.15 (medium), and 0.35 (large) – the impact of each of the independent variables upon their corresponding dependent variables are shown in Tables 5-16 through 5-18. Table 5-16 demonstrates that both usefulness and privacy and security concerns have a significant impact upon attitude, while the impact of trust and control is minimal. Turning to privacy and security concerns, no paths into this construct are large. While trust has a medium impact the remaining constructs (disposition to trust, PIIT, and control) have only a small influence. Finally, looking at usefulness, the effect of privacy and security is medium while that of control is small. Therefore, the four most dominant paths, in order of strength, are from privacy and security concerns and usefulness to attitude, privacy and security concerns to usefulness, and trust to privacy and security concerns.

Table 5-16: Effect Sizes of Antecedents of Attitude

R^2 (included) = 0.679	Trust	Usefulness	PSC	Control
R^2 (excluded)	0.677	0.508	0.473	0.661
F^2	0.01	0.53	0.64	0.06
Effect	none	large	large	small

Table 5-17: Effect Sizes of Antecedents of Privacy and Security Concerns

R^2 (included) = 0.236	Disp. Trust	Trust	PIIT	Control
R^2 (excluded)	0.221	0.112	0.212	0.222
F^2	0.02	0.16	0.03	0.02
Effect	small	medium	small	small

Table 5-18: Effect Sizes of Antecedents of Usefulness

R^2 (included) = 0.168	PSC	Control
R^2 (excluded)	0.008	0.147
F^2	0.19	0.03
Effect	medium	small

5.9 Saturated Model

Using the simplified model as the "base", a saturated model was developed and tested to investigate the possibility of the existence of additional relationships not previously included. The saturated model is not shown due to the fact that the excessive links make it somewhat unruly and convoluted. The saturated model contains 21 paths in total. While some of these paths were part of the original model, they have been reintroduced in the interests of completeness. All the hypothesized paths in the simplified model, and their corresponding coefficients, t-statistics, etc., for both the simplified and saturated model are shown in Table 5-19. The findings for the new paths created in the saturated model are shown in Table 5-20. There were essentially no differences in the hypothesized paths between the simplified model and saturated simplified model; and no new significant paths were noted.

Table 5-19: Summary of Findings for Saturated Model for Original Hypothesized Relationships

		Non-Saturated Model				Saturated Model				
Hyp.	Path	Beta	t-value	p-value	Val.	Beta	t-value	p-value	Val.	Δβ
H1	Usefulness -> Attitude	0.455	10.509	< 0.001	Supp.	0.451	9.842	< 0.001	Supp.	0.004
H2	PSC -> Attitude	-0.548	12.741	< 0.001	Supp.	-0.538	11.500	< 0.001	Supp.	-0.010
H3	PSC -> Usefulness	-0.407	7.345	< 0.001	Supp.	-0.393	5.804	< 0.001	Supp.	-0.014
H4	Trust -> Attitude	0.089	2.118	< 0.05	Supp.	0.093	2.305	< 0.05	Supp.	-0.004
H5	DT -> Trust	0.237	4.124	< 0.001	Supp.	0.227	3.889	< 0.001	Supp.	0.010
H7	Trust -> PSC	-0.372	5.844	< 0.001	Supp.	-0.374	5.898	< 0.001	Supp.	0.002
H8	DT -> PSC	-0.126	2.136	< 0.05	Supp.	-0.124	2.195	< 0.05	Supp.	-0.002
H11	PIIT -> Attitude	0.022	0.571	0.568	Rej.	0.032	0.810	0.419	Rej.	-0.010
H12	PIIT -> PSC	-0.149	2.760	< 0.01	Supp.	-0.135	2.162	< 0.05	Supp.	-0.014
H13	Control -> Attitude	0.125	3.977	< 0.001	Supp.	0.123	3.680	< 0.001	Supp.	0.002
H14	Control -> PSC	-0.120	2.125	< 0.05	Supp.	-0.121	2.113	< 0.05	Supp.	0.001
H15	Control -> Usefulness	-0.156	2.957	< 0.01	Supp.	-0.158	3.000	< 0.01	Supp.	0.002

Table 5-20: Summary of Findings for Saturated Model for New Relationships

From	To	Beta	t-value	p-value	Sig.	Status
PIIT	Disp Trust	0.113	1.675	0.095	n.s.	Rejected
PIIT	Trust	0.025	0.410	0.682	n.s.	Rejected
PIIT	Usefulness	0.099	1.666	0.097	n.s.	Rejected
DispTrust	Usefulness	-0.007	0.108	0.914	n.s.	Rejected
DispTrust	Attitude	0.032	0.909	0.364	n.s.	Rejected
Trust	Usefulness	-0.002	0.027	0.978	n.s.	Rejected
Control	Disp Trust	0.050	0.815	0.416	n.s.	Rejected
Control	Trust	0.075	1.214	0.226	n.s.	Rejected
Control	PIIT	0.057	0.931	0.353	n.s.	Rejected

5.10 Control Variables

Recall in Section 5.2 that various demographic and contextual variables were discussed. Six control models were created by introducing a control variable and establishing paths leading to all the constructs in the simplified model. The impact of these variables was assessed by comparing, for each construct, the variance explained between the uncontrolled model and each controlled model. The effects upon the R-squared values are reported in Table 5-21 and are marginal at best, which indicates that the control variables had very limited impact upon the explained variance. The one notable exception was the impact of gender upon PIIT suggesting that whether

individuals are male or female makes a difference in terms of personal innovativeness. This is further examined through MANOVAs in the post hoc analysis in the following section.

Table 5-21: Impact of Control Variables on R^2

	PIIT	DispTrust	Trust	PSC	Usefulness	Attitude
Uncontrolled Model	0.000	0.000	0.056	0.236	0.168	0.679
Gender	0.117	0.001	0.056	0.234	0.168	0.679
Age	0.021	0.001	0.059	0.233	0.169	0.679
Income	0.009	0.008	0.075	0.237	0.174	0.679
Education	0.009	0.022	0.057	0.236	0.169	0.681
ATM Use	0.007	0.011	0.056	0.235	0.170	0.679

In addition to analyzing the effect of demographic variables upon variance explained, the path coefficients between them and the model constructs were also explored. The results are given in Table 5-22.

Table 5-22: Impact on Control Variables on Model Constructs

		PIIT	Disp. Trust	Trust	PSC	Useful	Attitude
Gender	**Beta**	***-0.342***	-0.031	0.023	-0.060	-0.001	0.015
	t-value	***6.835***	0.514	0.396	1.080	0.022	0.468
	p-value <	***0.001***	n.a.	n.a.	n.a.	n.a.	n.a.
	Validation	***signif***	n.s.	n.s.	n.s.	n.s.	n.s.
Age	**Beta**	0.146	-0.036	-0.055	0.029	-0.027	-0.008
	t-value	1.943	0.603	0.965	0.532	0.495	0.241
	p-value <	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.
	Validation	n.s.	n.s.	n.s.	n.s.	n.s.	n.s.
Income	**Beta**	0.093	-0.087	***-0.136***	0.053	0.078	-0.013
	t-value	1.381	1.503	***2.322***	0.978	1.473	0.349
	p-value <	n.a.	n.a.	***0.02***	n.a.	n.a.	n.a.
	Validation	n.s.	n.s.	***signif***	n.s.	n.s.	n.s.
Education	**Beta**	-0.092	***-0.148***	-0.038	0.031	0.020	-0.051
	t-value	1.437	***2.487***	0.666	0.519	0.409	1.636
	p-value <	n.a.	***0.02***	n.a.	n.a.	n.a.	n.a.
	Validation	n.s.	***signif***	n.s.	n.s.	n.s.	n.s.
ATM Use	**Beta**	0.086	-0.105	0.005	0.024	0.047	0.020
	t-value	1.196	1.636	0.074	0.388	0.824	0.561
	p-value <	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.
	Validation	n.s.	n.s.	n.s.	n.s.	n.s.	n.s.

Looking at these control variables, there is very little to report. Age and ATM use demonstrated no significant impact. Although in looking at age, the number of respondents 45 and older was extremely low (only 8) thereby limiting the ability to draw any supportable conclusions. In keeping with the results from Table 5-21 and the subsequent MANOVAs (see Section 5.11), gender was shown to have a significant effect

upon PIIT. Income had a significant negative impact upon trust, as did education upon disposition to trust. In the case of the former, this would suggest that those with higher incomes place less trust in their banks than lower wage earners. Trying to explain the causality behind this correlation is pure speculation at this point but may be worth pursuing to explore the underlying reasons behind this phenomenon.

While the significant negative influence of education on disposition to trust suggests that those with higher levels of education possess a lower innate "ability" to trust, given the limited breadth of education levels investigated, this may be a somewhat spurious conclusion. Like the correlation of higher income and lower trust, suggesting causality is mere speculation but, again, it does suggest an area of further research, or at least a review of the extant literature to see if this phenomenon has been investigated and/or empirically demonstrated.

5.11 Post Hoc Analysis

In addition to examining the proposed model as a whole using PLS, recall that another component of this research was to examine the impact upon attitude of control and voluntariness acting simultaneously (see Table 4-1). To accomplish this, an ANOVA test was run with attitude mean as the dependent variable and scenario as the fixed factor.

The post hoc Bonferroni test (Table 5-23) shows, at a significance level of $p = 0.05$, that the attitude means between IBC and ISC are significantly different, as are the attitude means between IBC and VSC. Interestingly, the scenario in which attitude was the highest (mean = 4.674) was ISC, in which the consumer shared control of their biometric information, but participation was mandatory. Possible reasons behind this finding are discussed in Chapter 6. VSC had the second highest attitude score (mean = 4.459), VBC was third (mean = 4.319), and IBC was a distant fourth (mean = 3.805) (see Table 5-24 And Figure 5-3).

Table 5-23: Post Hoc Bonferroni Test of Attitude Mean for the Scenarios

Scenario	Scenario	Mean Difference	Std. Error	Sig.
IBC	ISC	-.8685*	.24901	.003
	VBC	-.5142	.23594	.181
	VSC	-.6538*	.24045	.042
ISC	IBC	.8685*	.24901	.003
	VBC	.3543	.25274	.973
	VSC	.2148	.25695	1.000
VBC	IBC	.5142	.23594	.181
	ISC	-.3543	.25274	.973
	VSC	-.1395	.24430	1.000
VSC	IBC	.6538*	.24045	.042
	ISC	-.2148	.25695	1.000
	VBC	.1395	.24430	1.000

*Significant at the 0.05 level

Table 5-24: Descriptive Statistics for the Four Scenarios

Scenario	Mean	Std. Deviation	N
IBC	3.805	1.516	77
ISC	4.674	1.373	59
VBC	4.319	1.371	72
VSC	4.459	1.476	67
Total	4.286	1.468	275

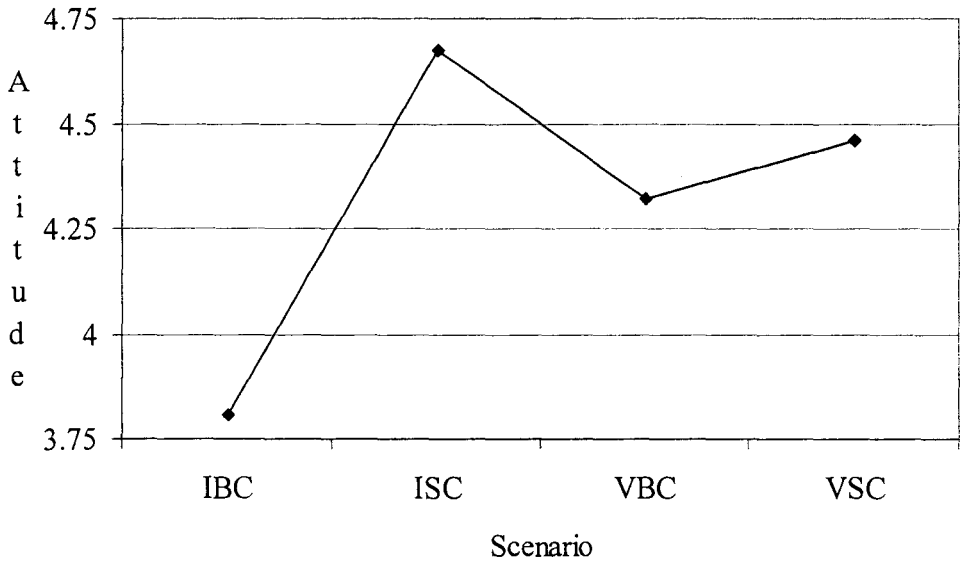


Figure 5-3: Mean of Attitude for the Four Scenarios

In the interests of completeness, five MANOVAs were also run using the five control variables (ATM Use, Education Level, Income, Age, and Gender) as the fixed factors and all the means of the reflective constructs as the dependant variables. While no hypotheses were developed with respect to these control variables, their analysis may provide insights that could suggest areas warranting further investigation. The results of the five MANOVAs are summarized in Table 5-25.

Table 5-25: MANOVA of Control Variables

	ATM Use	Education	Income	Age	Gender
Disposition to Trust	n.s.	n.s.	n.s.	n.s.	signif
PIIT	n.s.	n.s.	n.s.	signif[1]	signif
Trust	n.s.	n.s.	n.s.	n.s.	n.s.
Usefulness	n.s.	n.s.	n.s.	n.s.	n.s.
Attitude	n.s.	n.s.	n.s.	n.s.	n.s.

[1]significant difference demonstrated between group 1 (18-24) and group 3 (35-44)

There were no significant differences amongst the four ATM frequency of use categories. One could speculate that there might have been a significant difference in usefulness and/or attitude for this control variable in that people that use ATMs more frequently might have ascribed greater value to this identity authentication method, versus the current system of debit cards and passwords, and therefore demonstrated a more positive attitude towards it. However, this might be mitigated by the influences of control given that comments from the open-ended questions (see Section 5.12) mentioned that

having shared control and being required to carry a smart card was not that much more convenient than the present system. Subsequent analysis did not demonstrate any significant interaction effects between control and ATM use.

Similarly, there were no differences for education or income. Given the nature of the sample being comprised of only two closely related groups with respect to education level, the fact that there are no significant differences is not surprising. Looking at income, there might be literature that suggests higher income earners show a higher propensity to be risk lovers, more open to innovative technologies, etc., but examination of these aspects is beyond the present scope of this research and, even if that is the case, the results shown here would indicate otherwise. Likewise, it may seem reasonable to suggest that those with higher incomes may have more assets to protect and, therefore, might be more inclined to view biometric identity authentication in a more favourable light, and/or as more useful, than lower wage earners. Despite the logical appeal of this notion, the outcome of the tests performed do not support this conjecture.

Moving to age, while five of the constructs show no significant difference, PIIT does. What is even more interesting is that the 35-44 age bracket has a higher mean (5.267) than the 18-24 age bracket (4.638). This flies in the face of other research that demonstrates that younger generations are more comfortable with technology than older generations (Larsen and Sørebø 2005). Perhaps the reason for this finding is due to the how the respondents evaluated their PIIT. In other words, they may have been assessing their level of PIIT relative to their peer group (in terms of age) as opposed to the population at large. For example, in the 18-24 age bracket the respondents may have felt that, even though they have the latest technological devices, relative to their friends they adopted this technology later. While this may be true, if their adoption of technology was objectively compared to that of the 35-44 age bracket, it is quite possible that they are, in fact, much more "wired" and advanced than the 35-44 year olds. Conversely, the 35-44 year olds that took the survey may see themselves as much more advanced than their peers in the same age braeket and responded accordingly while, when compared to 18-24 year olds, they are actually lagging behind. Unfortunately, there is no way that we can objectively assess each respondent's PIIT and we therefore have to rely on their subjective assessment which, as stated, may very well be clouded by their comparison to their age group as opposed to society at large.

Finally, looking at gender, PIIT ($F = 35.759$, $p = 0.000$) is significantly different between males and females. It is higher for males than females. The mean of PIIT for males is 5.205 and it is 4.409 for females. Previous research examining these dimensions has demonstrated similar results (Larsen and Sørebø 2005), so these findings simply add further support.

5.12 Analysis of Open Ended Questions

The analysis consisted of examining the first two questions, dealing with advantages and concerns respectively, in a similar manner to the answers received from the qualitative survey as discussed in Chapter 3, Section 3.3.1.

The results for advantages are given in Table 5-26. The top three advantages given in all but VSC are security, usefulness, and ease of use. While the values for ease of use are small, the fact that it is mentioned at all is somewhat surprising given that respondents were simply given a scenario and could not actually try out a biometric reader. Perhaps the respondents inferred ease of use based upon the description of how the hardware would work: "you must place your index finger on a biometric scanner which instantaneously verifies a match of your fingerprint with the electronic version stored at the bank", which was essentially the same in each scenario. The percentage results of the top three advantages in IBC and VBC are virtually identical, while they are roughly the same in ISC and VSC. In IBC and VBC, the bank controls the information. As such, it makes intuitive sense that the advantage of security would be mentioned by just under 50% of the respondents while being mentioned as an advantage 74.6% and 64.2% of the time for ISC and VSC respectively where control is shared such that, if the bank system is breached, your security is not compromised to the same degree. The reverse is true with respect to the advantage of usefulness. Again, this is not surprising since when the bank is solely responsible for the biometric identifier, there is no need to carry a smart card as is the case in ISC and VSC. This demonstrates the tradeoff required between the advantages of security and usefulness when looking at control.

Table 5-26: Analysis of Qualitative Question Regarding Advantages/Benefits

	IBC		ISC		VBC		VSC	
	Number	%	Number	%	Number	%	Number	%
Security	36	46.8	44	74.6	35	48.6	43	64.2
Usefulness	45	58.4	16	27.1	43	59.7	21	31.3
Ease of Use	5	6.5	5	8.5	6	8.3	4	6.0
None	3	3.9			2	2.8	8	11.9
Other	1	1.3	3	4.1			1	1.5
Total Respondents	77		59		72		67	

Turning to concerns, a similar pattern emerges as is shown in Table 5-27. As one's biometric template resides exclusively with the bank in scenarios IBC and VBC, security and privacy concerns are greater than in scenarios ISC and VSC where control is shared. Although the percentage of respondents that mentioned inconvenience, technical issues, and safety as concerns was into double digits in some cases, there is no discernable pattern amongst the scenarios beyond those noted for security and privacy.

Table 5-27: Analysis of Qualitative Question Regarding Concerns

	IBC		ISC		VBC		VSC	
	Number	%	Number	%	Number	%	Number	%
Security	35	45.5	18	30.5	33	45.8	24	35.8
Privacy	35	45.5	20	33.9	37	51.4	28	41.8
Inconvenience	13	16.9	9	15.3	4	5.6	7	10.4
Technical Issues	8	10.4	7	11.9	11	15.3	8	11.9
Safety	7	9.1	2	3.4	3	4.2	7	10.4
Hacking Implications	1	1.3	1	1.7	2	2.8	2	3.0
None	3	3.9	1	1.7	3	4.2		
Cost	3	3.9						
Health Issues							2	3.0
Other			1	1.7	3	4.2		
Total Respondents	77		59		72		67	

Finally, when the percentages of the top two advantages are combined, for comparison purposes, with the percentages of the top three concerns, the results are as depicted in Table 5-28. Once again, groupings become immediately evident based upon the aspect of control. While in scenarios IBC and VBC the advantage of security is essentially equal to security concerns, in scenarios ISC and VSC, the advantage of security is roughly twice that of security concerns. Moving on to privacy, virtually no one cited it as an advantage; but in terms of it being a concern, the values in scenarios ISC and VSC are approximately 10 percentage points lower than in scenarios IBC and VBC respectively. However, this higher degree of concern appears to be mitigated by usefulness being cited as an advantage about twice as often in scenarios IBC and VBC than in ISC and VSC respectively. Once again these results illustrate the tradeoff when looking at where control resides. Bank control provides higher value in terms of perceived usefulness; but that is mitigated by the higher "costs" of privacy and security concerns. Conversely, shared control is associated with lower privacy and security concerns, but that is offset by lower perceived usefulness.

Table 5-28: Comparison of Advantages/Benefits With Concerns

	IBC		ISC		VBC		VSC	
	Adv.	Concerns	Adv.	Concerns	Adv.	Concerns	Adv.	Concerns
Security	46.8	45.5	74.6	30.5	48.6	45.8	64.2	35.8
Privacy		45.5	1.7	33.9		51.4	1.5	41.8
Usefulness/ Inconvenience	58.4	16.9	27.1	15.3	59.7	5.6	31.3	10.4
Total Respondents	77		59		72		67	

Chapter 6 Discussion and Conclusions

This chapter discusses the findings of this research and their implications. The first three sections review the findings of the three studies and their associated research questions posed at the beginning of this dissertation in Section 1.2. Second, the academic and practitioner contributions provided by this empirical investigation are discussed. Third, limitations of this research are summarized. Finally, potential avenues for future research are presented.

6.1 Study 1

Research Question: What avenues of exploration does the Canadian banking industry consider to be most salient with respect to consumer perceptions of biometric authentication technology?

There appeared to be consensus that no Canadian bank would unilaterally pursue biometric authentication technology. In other words, this form of authentication would be an industry-wide initiative. As such, of tantamount importance to the banks was the identification of what consumers' primary concerns were regarding this method of gaining access to their financial data and assets, as well as what customers perceived as the potential benefits of biometrics. Armed with this information, the banks would be in a position to at least initially evaluate the viability of deploying biometric authentication. For example, if concerns significantly outweighed perceived benefits in terms of both number of mentions and the strength of the objections, then perhaps biometric authentication should not be considered as an option in the short term. Additionally, should biometrics be seen as a practicable option by consumers, this information could be used to address customer concerns, via educational initiatives, while simultaneously leveraging the perceived benefits.

There was complete consensus regarding the top two contexts that should be examined: control and voluntariness. Recall that the aspect of control was operationalised as the bank retaining one's complete biometric template versus the bank only retaining half of the template while the other half was held by the customer in the form of a "smart card". This was deemed to be important since in the former instance the aspect of convenience is increased relative to the latter scenario; however, this increase in convenience may be perceived as coming at the price of reduced privacy. The banks' curiosity with respect to the aspect of voluntariness is self-explanatory; if making biometric authentication mandatory could result in significant consumer backlash, then why pursue this approach.

6.2 Study 2

Research Question: What do consumers perceive as the benefits of, and what are their concerns with, the deployment of biometric authentication technology within the Canadian banking industry?

In terms of concerns, security of one's biometric information received the most number of mentions by a considerable margin suggesting that any rollout of this technology by the banks will have to come with assurances to consumers that the safeguards surrounding this data is well beyond adequate. The second most frequently mentioned concern was the inconvenience of not being able to have someone else doing your banking. While the sharing of one's debit card and PIN is highly discouraged, the fact remains that it would appear to be acceptable practice among a significant portion of the population. Even those that do not share their banking information as a rule may find the need for someone else to do their banking should they be temporarily incapacitated. Depending upon the magnitude of this practice, and whether its occurrence is increasing or decreasing, it could be a major impediment to the acceptance and ultimate use of biometric authentication for accessing one's bank account(s).

The next two concerns got almost the same amount of mentions with function creep ending up slightly ahead of privacy. Recall that function creep is defined as the use of one's personal information beyond the initial intended use without the individual's permission and, as such, is essentially an element of privacy. However, due to the frequency of it being cited as a concern, it was deemed appropriate to highlight its importance in the eyes of consumers. It would appear that not addressing the issue of privacy would hinder the implementation of biometric authentication technology. Perhaps legislation along the lines of Canada's PIPEDA (Personal Information Protection and Electronics Documents Act) that addresses biometrics may help allay people's privacy concerns.

The potential for physical harm, relative to the existing practice of a debit card and PIN, was the fifth most cited concern. While viability tests can be connected to biometric readers insuring that the person is alive, the fact remains that would-be criminals now need the person as opposed to an inanimate object and a PIN. Even though this was mentioned by just over 10% of the survey participants, the potential of sustaining physical injury or being abducted may be insurmountable concern for some people.

Two primary benefits were identified: increased security and convenience. In light of the two most mentioned concerns being security and inconvenience, this may seem contradictory, but this may not necessarily be the case, at least with respect to security. It seemed to be acknowledged that biometric authentication does have the potential to be more secure than the present method of accessing one's bank account essentially based upon the belief that each individual's fingerprint is unique. However, this would appear to be based upon the caveat that the biometric information itself is adequately safeguarded.

With respect to convenience and inconvenience, this is more paradoxical as people realize the benefit of not needing a card or PIN while at the same time recognizing the inability to have someone else do their banking should the need arise, and vice versa. Given that these two points are diametrically opposed and, therefore, there is no middle ground, considerable further research, in terms of population coverage, will be necessary to adequately assess which aspect of convenience is more desirable. In addition, the findings of such a survey may be relevant at that point in time only as shifts in the proportion of age groups, and the associated demographics of marital status, dependent children, mobility, etc., could significantly influence the results.

In conclusion, this study demonstrates that the subject of biometric authentication elicits considerable conflict in the minds of consumers as they appear to wrestle with both the positive and negative aspects of the technology. Given the highly personal nature of biometrics relative to most other technologies, it also seems to induce an almost visceral reaction, especially from those opposed to its use. Whether this adamant resistance will recede with improvements to the technology and/or increased deployment remains to be seen.

6.3 Study 3

Recall that Study 3 posed three research questions. These will be individually examined over the next three sections.

6.3.1 Research Question 1

Question #1: Within the context of biometrics being used by Canadian financial institutions for identity authentication, what are the factors that directly shape consumer attitudes towards this method of authentication?

Related Hypotheses:

H1: Individuals with a higher degree of perceived usefulness will demonstrate a more positive attitude towards adopting biometric authentication technology for accessing their bank account(s).

H2: Individuals with a higher degree of privacy and security concerns will demonstrate a less positive attitude towards adopting biometric authentication technology for accessing their bank account(s).

H3: Individuals with a higher degree of privacy and security concerns will demonstrate a lower degree of perceived usefulness towards biometric authentication technology for accessing their bank account(s).

H4: Individuals with a higher degree of trust in their bank will demonstrate a more positive attitude towards adopting biometric authentication technology for accessing their bank account(s).

H7: Individuals with a higher degree of trust will demonstrate a lower degree of perceived privacy and security concerns with respect to using biometric authentication technology for accessing their bank account(s).

While all of these hypotheses were statistically supported, one (H4) demonstrated a lower confidence level than the other 4. Privacy and security concerns had a significant negative impact upon both attitude (H2: $\beta = -0.548$, p-value < 0.001) and usefulness (H3: $\beta = -0.407$, p-value < 0.001). The effect size of privacy and security concerns upon attitude and usefulness was large and medium respectively (see Tables 5-16 and 5-18); and examining the responses to the qualitative open-ended questions gives further credence to the argument that these are definitely a top-of-mind consideration for consumers as the majority of people that chose to express their concerns mentioned either the issue of privacy or security, or both. While the nature of the context examined in this research (i.e. protection of financial assets) would obviously have an influence on how people answered both the survey items and the open-ended questions, it seems that it may be prudent to educate effected parties when biometric identity authentication is being considered in any context given the weight people ascribe to the joint issues of privacy and security when dealing with such personal information. Subsequent sections will deal with these concepts in terms of further research, limitations of this research, and practical implications.

Trust was found to have an impact upon attitude both directly and indirectly. While the influence of trust on attitude was significant (H4: $\beta = 0.089$, p-value < 0.05), it appears to have a more indirect influence through privacy and security concerns (H7: $\beta = -0.372$, p-value < 0.001). This is supported by the findings of the effect size calculation of trust upon attitude, and privacy and security concerns (see Tables 5-16 and 5-17). With respect to the former, it is negligible ($f^2 = 0.01$) whereas in the case of the latter, it has a medium effect ($f^2 = 0.16$). This suggests additional avenues of research are needed to further examine this mediation effect across a variety of scenarios and contexts. Only three responses to the open-ended questions mentioned the issue of trust in one's bank. Interestingly, the two respondents that said they do not trust their bank with this information were in ISC and VSC in which there is shared control of the biometric information. One respondent in VSC said that while they trust their bank, they do not necessarily trust "some individuals who can abuse it". This is an interesting distinction that should be explored further.

Given the support for the hypothesis that usefulness influences attitude (H1: $\beta = 0.455$, p-value < 0.001), it appears that consumers understand and appreciate the value of using biometrics for identity authentication at their banks. While the effect sizes (see Tables 5-16) of usefulness upon attitude ($f^2 = 0.53$) and privacy and security concerns upon attitude ($f^2 = 0.64$) are large according to Cohen's (1998) operational definition, the value of the latter is more than that of the former. Perhaps this suggests that the positive effect of usefulness upon attitude is outweighed by the negative effect of privacy and security concerns. This was also a theme in the analysis of the open-ended questions. These findings harp back to the previous discussion in Chapter 2 revolving around the tradeoffs people make between perceived benefits and perceived consequences, particularly with respect to privacy. It has been referred to previously as the

"personalization-privacy paradox" (Awad and Krishnan 2006) and a "privacy calculus" (Culnan and Armstrong 1999).

6.3.2 Research Question 2

Question #2: What are the innate individual traits that influence consumers' perceptions about biometric authentication and, ultimately, their attitude towards biometric identity authentication for financial transactions?

Related Hypotheses

H5: Individuals that have a greater disposition to trust will demonstrate a higher degree of trust towards their bank.

H6: Individuals with a high risk propensity will demonstrate a lower degree of perceived privacy and security concerns with respect to using biometric authentication technology for accessing their bank account(s).

H8: Individuals that have a greater high disposition to trust will demonstrate a lower degree of perceived privacy and security concerns with respect to using biometric authentication technology for accessing their bank account(s).

H9: Individuals with a high risk propensity will demonstrate a more positive attitude with respect to using biometric authentication technology for accessing their bank account(s).

H10: Individuals with a high degree of PIIT will demonstrate a higher degree of risk propensity.

H11: Individuals with a high degree of PIIT will demonstrate a more positive attitude with respect to using biometric authentication technology for accessing their bank account(s).

H12: Individuals with a high degree of PIIT will demonstrate a lower degree of perceived privacy and security concerns with respect to using biometric authentication technology for accessing their bank account(s).

Only four of the seven hypotheses proposed above were significant. In addition, and as previously discussed, while the path from PIIT to risk propensity was significant (H10: $\beta = 0.307$, p-value < 0.001), the hypothesized paths emanating from risk propensity to attitude (H9: $\beta = 0.047$, p-value n.s.) and from risk propensity to privacy and security concerns (H6: $\beta = 0.064$, p-value n.s.) were not, such that risk propensity was dropped in the simplified model. Previous research has demonstrated that risk propensity does have a significant impact upon risk perceptions across a wide variety of situations. Perhaps in the context of using biometrics for identity authentication at one's bank, the perceived risks are too great to be overcome by innately risk-loving consumers. Examining the impact of risk propensity upon risk taking behaviour, you may recall that while Chen and He (2003) demonstrated that the former did have an impact upon the latter, Sitkin and Weingart (1995) did not. The results of this research add support to the findings of Sitkin and Weingart (1995).

The fact that PIIT does have a significant effect upon risk propensity adds support to the contention of Agarwal and Prasad (1998) that innovators embrace risk. However, while personal innovativeness traits have been demonstrated to influence online banking adoption (Lassar et al. 2005), the results obtained in this study suggest that this phenomenon does not carry over to the realm of using biometrics for identity authentication at one's financial institution given the non-significant path from PIIT to attitude (H11: $\beta = 0.022$, p-value n.s.). That being said, the effect of PIIT on privacy and security concerns is significant (H12: $\beta = -0.149$, p-value < 0.01), suggesting that the influence of PIIT upon attitude is fully mediated by privacy and security concerns.

Disposition to trust had a significant positive effect upon trust (H5: $\beta = 0.237$, p-value < 0.001) which is not at all surprising given the multitude of previous empirical evidence demonstrating similar results. In addition, like PIIT, disposition to trust had a significant negative influence upon privacy and security concerns (H8: $\beta = -0.126$, p-value < 0.05). This result is not surprising, although one may have expected larger effect sizes (see Tables 5-17). The effect sizes of disposition to trust and PIIT on privacy and security concerns were only 0.02 and 0.03 respectively. Nonetheless, it does imply that privacy and security concerns of biometric use for identity authentication to obtain access to one's bank account(s) are somewhat mitigated for individuals that are more trusting in nature and/or more innovative in terms of trying new technologies. In terms of qualitative aspects, there was essentially nothing mentioned with respect to disposition to trust, innovativeness, or risk propensity. There were a few comments that it sounds interesting, is the wave of the future and the like, but nothing that could be definitively attributed to a respondent giving any thought to their underlying personality traits.

6.3.3 Research Question 3

Question #3: How will consumer control of their biometric information and program voluntariness, acting alone and simultaneously, impact these factors?

Related Hypotheses

H13: In circumstances where individuals have a higher degree of control over their biometric information, attitude towards the use of this technology for accessing their bank account(s) will be more positive.

H14: In circumstances where individuals have a higher degree of control over their biometric information, privacy and security concerns towards the use of this technology for accessing their bank account(s) will be reduced.

H15: In circumstances where individuals have a higher degree of control over their biometric information, usefulness with respect to the use of this technology for accessing their bank account(s) will be reduced.

H16: In circumstances where biometric identity authentication is voluntary, individuals' attitudes towards the use of biometric identity authentication technology for accessing their bank account(s) will be greater than in circumstances where it is not voluntary.

The results of the PLS model demonstrate that control does have a significant positive impact upon attitude, and a significant negative impact upon privacy and security concerns and usefulness thereby supporting hypotheses 13, 14, and 15. Although the effect size was small ($f^2 = 0.06$) the hypothesis that a higher degree of control positively influences attitude towards using biometrics for identity authentication was supported (H13: $\beta = 0.125$, p-value < 0.001). The effect size of control upon privacy and security concerns was also small ($f^2 = 0.02$); nonetheless the path was significant (H14: $\beta = -0.120$, p-value < 0.05). This supports the notion held by a variety of scholars that control is central to the concept of privacy.

As previously mentioned, when information is held by another party, control refers to control over the data itself and how it is used. With shared control of one's biometric, the biometric information held by the bank is incomplete. It is therefore useless unless it is combined with the biometric information held by the consumer in the form of a smart card. This implies that, even if the bank wished to share a customer's biometric information, they are not able to do so. As a result, the two aspects of control as outlined above are satisfied. More specifically, because the biometric information is jointly held, the customer has control over the data; and because the information the bank has is useless without the customer's smart card, it cannot be used by the bank for other purposes, such as sharing it with government authorities. Whether the consumer actually makes these inferences is speculative without further qualitative research to assess what consumers are actually thinking; but the finding that increased control negatively affects privacy and security concerns does provide support for this notion, especially since this result was demonstrated through both PLS and the answers to the qualitative questions. In the case of the latter, the mentioning of privacy and security concerns was approximately 10% lower when the biometric information was shared versus when it was held by the bank alone. In terms of usefulness, running the model through PLS demonstrated that increased control has a significant negative impact upon usefulness. As with privacy and security concerns, this finding was further supported by the results of the answers to the qualitative questions. When the biometric information was maintained by the bank alone, usefulness was mentioned as a benefit roughly 60% of the time; but when the biometric information was jointly held such that control was increased, this figure was essentially halved. This suggests that it is inconvenient to carry a card, which is what is required when control is shared.

Also as hypothesized, control negatively influences perceptions of usefulness (H15: $\beta = -0.156$, p-value < 0.01). Once again, the effect size is small ($f^2 = 0.03$). However, when this finding is examined in conjunction with the results of the open ended questions in which the respondents acknowledged the tradeoff between usefulness and privacy and security concerns within the context of control, it adds further support to the notion that, when determining whether or not to use biometric authentication technology, consumers simultaneously evaluate opposing factors.

Whether participation in the biometric identity authentication program was mandatory or voluntary had no significant effect upon attitude, thereby rejecting the hypothesis (H16: β = 0.047, p-value n.s.). This was surprising as the aspect of voluntariness may be construed as a form of de facto control over the information one provides and, therefore, it seemed logical to presume that this would impact attitude.

However, when voluntariness was combined with control thereby creating the four scenarios, its impact was significant. Interestingly, the scenario with the highest attitude score (mean = 4.674) was ISC. VSC had the second highest attitude score (mean = 4.459); and the attitude score (mean = 4.319) was third highest in VBC. Not surprisingly, the lowest attitude score (mean = 3.805) came in IBC. Running a post hoc Bonferroni test shows that while there is no significant difference in the attitude means between ISC and VSC and between IBC and VBC, there is a significant difference in the attitude means between IBC and ISC and between IBC and VSC. The fact that ISC had the highest attitude score is somewhat surprising given that participation was mandatory. As to why this is the case is subject to speculation and debate. Perhaps people find the *requirement* of surrendering biometric information to access their bank accounts so egregious, that adding the ability to exercise some control makes it that much more palatable. This may very well be the case since, when the program is voluntary (VBC and VSC), the aspect of consumer control appears to be virtually insignificant given the very close attitude scores between these two scenarios. In the latter case, maybe the fact that the entire program is voluntary gives the consumer the perception of de facto control in the sense that they don't have to use it in the first place such that anything (i.e. using a smart card to establish shared control) beyond the initial choice of whether or not to participate is essentially considered redundant in the minds of consumers.

6.4 Contributions

The goal of this research was to develop an initial understanding of the factors that may influence consumer attitudes towards biometric identity authentication methods at the ATMs of their financial institutions. The findings make several contributions to both theory and practice as is outlined in the following sections.

6.4.1 Contributions to Theory

From an academic perspective, this research makes important contributions by developing and validating a research model for consumer attitudes towards the use of biometric identity authentication in financial transactions. This acceptance was also tested under various conditions (i.e. control and voluntariness) using a scenario based approach. The empirical results of this research represent an important first step in understanding consumers' attitudes towards using biometrics as a means of identity authentication in financial transactions. Previous research appears to have either developed a proposed framework and simply explored the acceptability of various biometric measures, or examined the acceptability of various types of biometrics across various contexts without considering possible antecedents.

While the proposed model was developed with a specific use of biometric identity authentication in mind, it could be adapted to assess other applications of biometric technology. In fact, investigating other contexts could provide valuable insight as to whether the influence of control, usefulness, and privacy and security concerns are relatively consistent across different situations and therefore systemically driven by the technology itself, or significantly different thereby suggesting that the application being considered is the driver.

The proposed model demonstrated that the positive effect of usefulness upon attitude is countered by the negative influence of privacy and security concerns. This dichotomy is analogous to Awad and Krishnan's (2006) "personalization-privacy paradox" and Culnan and Armstrong's (1999) "privacy calculus". The research presented here suggests that perhaps there is a further dichotomy in the context under examination. Given the nature of the interplay between privacy and security and the confusion surrounding the distinction between the two, combined with the inextricability of the two concepts within the realm of using biometric identity authentication to access one's bank accounts (i.e. sacrificing privacy is required to beget increased security), they have been combined in this research thereby suggesting the existence of a "privacy-security paradox/calculus". The results of the analysis of the qualitative questions add further support to this notion.

Given the demonstrated significant impact of control on not only attitude but also on the antecedents of privacy and security concerns and usefulness, this research suggests the possibility that perhaps the interplay of these concepts, with regard to biometric authentication, is a lot more complex than originally envisioned. Based upon the SEM analysis and the qualitative answers, increased control begets a more positive attitude towards biometrics as well as reduced privacy and security concerns; but this comes at the expense of reducing the benefit of perceived usefulness. However, per the qualitative answers, increasing control also increases the benefit of security. There is no privacy benefit in any context as the whole premise of biometric authentication is the surrendering of very private information for increased security.

6.4.2 Contributions to Practice

While the proposed model was driven by theory, the scenarios were developed through both the examination of the extant literature and extensive discussions with personnel from three of the five major Canadian banks. This collaboration between researchers and practitioners should leverage the usefulness of the findings in both the academic and practitioner environments.

From the perspective of the practitioner, there is a considerable amount of information that can be gleaned from the findings and incorporated into initiatives to introduce biometric identity authentication. While the research presented here examined the context of access to one's information and assets at their financial institution, some of the findings may very well be applicable to other contexts, as will be discussed.

The significant negative influence of privacy and security concerns on both attitude and usefulness suggest that the threat of biometric information being compromised, either inadvertently (i.e. a security breach) or intentionally (i.e. being shared with other entities) is a top-of-mind issue for consumers. Banks wishing to employ biometric authentication should target their marketing campaigns at educating consumers with respect to the superiority of biometric technologies relative to other forms of identity authentication. It would also seem prudent to address any concerns about what is actually stored (e.g. encrypted mathematical "template" of the biometric measure as opposed to the actual biometric image itself) and the implications this has even if the information is compromised (i.e. the stored mathematical template is useless even without shared control as it cannot be reverse engineered into the original biometric measure).

While the answers to the open-ended questions suggest that the Canadian banking context is very relevant, a few comments expressed a general concern with respect to the perception that there might be general movement towards this method of identity authentication. When this notion is combined with further comments from the qualitative questions regarding distrust of the government and potential "big brother" scenarios, and the fact that some nations are leaning towards the use of biometrically-enabled government issued documents such as passports, perhaps a more overarching education agenda is warranted. In other words, perhaps the issue of education with respect to biometric identity authentication should become a national public policy initiative.

Aside from the need to educate the public about the nature of what is actually captured and stored in a system that employs biometric identity authentication, the open-ended questions also suggest that there could very well be a general lack of understanding of the basics of how biometric technology works. The biggest misconception in this regard would seem to be the potential of getting one's body parts removed by criminals such that they can get access to their victim's account(s) at will, while leaving said victim disabled. One argument put forward was that a biometric identity authentication system is less desirable than our present debit card and password system because in the case of the former, they can simply take your hand to get access to your money. However, in the case of the latter, the criminal would find it harder as they would have to torture you in order for you to give up your password, they couldn't simply "steal" it. This argument can be easily countered by the simple fact that biometric reading devices are equipped with viability sensors. In other words, and quite possibly in anticipation of such an eventuality, biometric readers will not work unless they detect signs of life. Nonetheless, recall that the potential for physical harm was mentioned as a concern in both the second study and the open-ended questions in the third study. Therefore, given the personal contact required to perpetrate theft of one's financial assets when they are safeguarded by biometrics, as opposed to the physically non-invasive theft of one's debit card and/or PIN, this type of identity authentication system may be a non-starter for consumers with concerns for their physical safety.

While the effect sizes of both privacy and security concerns and usefulness are large, it is still bigger for privacy and security concerns. Furthermore, upon examining the responses to the open ended questions, relative to bank control, shared control reduces (but does not eliminate) privacy and security concerns while simultaneously providing increased security benefits but decreased convenience benefits. Therefore, any initiative to roll out biometric identity authentication in the context of access to one's bank accounts must seek to minimize security and privacy concerns, as discussed above, while emphasizing the benefits. Therefore, irrespective of the whether control is shared or enrollment is voluntariness, and aside from addressing consumer misconceptions about biometric authentication technology, the banks must be able to demonstrate to the public that they have instituted sufficient and appropriate safeguards and educate consumers as to how and why they will work at ensuring their privacy and security, while providing a better alternative to the present system of bank cards and PINs.

Another issue cited by respondents in terms of inconvenience is the inability to use biometrics anywhere except the branches of *their* financial institutions. In other words, consumers may be more accepting of this technology if it could be used essentially wherever debit cards are presently used thereby altogether eliminating the need for the latter. This implies a tremendous upfront cost to the financial institutions, the infrastructure suppliers (i.e. Interac), the merchants, etc. in a variety of areas such as hardware, software, and training. Depending upon the importance of this in the minds of consumers, this could stop dead any thought of using biometrics for the purposes of accessing one's bank account(s) in the near future.

The final issue mentioned within the realm of usefulness is that of sharing ATM banking duties. It would seem logical to presume that joint accounts would have joint biometric identity authentication abilities. However, some people were concerned that if they are unable to do their personal banking, biometrics would make it impossible for them to get someone else to do it. Such is obviously not the case with the present system. While the practice of giving other people access to your bank account is highly discouraged (especially given studies showing that IDF is perpetrated by known acquaintances), if it is rampant it could prove a major stumbling block in terms of adoption of biometrics simply because you can't "lend" someone your biometric so that they can do your banking for you.

While the effect size of the personality trait personal innovativeness in the domain of information technology upon privacy and security concerns was quite small, it was nonetheless significant. Therefore, the identification of customers that tend to be more adventurous when it comes to trying new technologies would be key as marketers could then be more efficient and effective in deploying their resources to better target these segments and leverage any influence they might have on later adopters of technology.

The impacts of control and voluntariness, especially when looked at simultaneously as was done in this research, provide some valuable insights for

practitioners. The huge and significant disparity in attitude between IBC (mandatory and bank control: mean = 3.805) and ISC (mandatory and shared control: mean = 4.674) suggest that if Canadian banks make this form of identity authentication mandatory, then control should be shared unless they want to experience widespread dissent and various forms of customer backlash. This is a key finding for the banks as they are of the opinion that if they were to pursue this initiative they would make it mandatory for new customers and grandfather existing customers giving them a specified timeframe over which they would have to migrate to this form of identity authentication. This is due to the fact that they do not want to have to incur the costs of two access systems any longer than absolutely necessary. Conversely, if the use of biometrics is voluntary, it would appear that the issue of control becomes moot as there is no significant difference between VBC (voluntary and bank control: mean = 4.319) and VSC (voluntary and shared control: mean = 4.459). Per the previous point, making biometric identity authentication voluntary is an unlikely scenario. Nonetheless, if they do end up following this path, this insinuates that they can dictate where control resides, which means they will probably adopt whatever is the least expensive.

6.5 Limitations

As with any research, this research contains several limitations. First, although the qualitative study that examined privacy and security concerns does not suffer from the same limitation, the respondents used for the final survey came from a pool of MBA students at two universities in southern Ontario such that its generalisability to society at large is limited from various standpoints such as socioeconomic status, age, etc. "However, the majority of e-Commerce research utilizes undergraduate and/or MBA students as their subject pool (Grabner-Kräuter and Kaluscha 2003). From the student groups, MBA students are preferred in this context as they typically make better decisions (Remus 1989), [and] have more varied backgrounds" (Hassanein and Head 2007, p.705). This variation should extend beyond education and experiences and include income level and age; these factors will be further enhanced by the fact that respondents were both part-time and full-time MBA students.

Second, this study was conducted in Canada which results in three limitations. First, biometric authentication is virtually non-existent and there are no national identity cards. The absence of national identity cards could possibly heighten people's misgivings with respect to privacy concerns and the issue of "function creep" and the specter of "big brother" relative to those countries that do have national identity cards. Further to the point that biometric authentication is not very prevalent in Canada means that in the scenarios people had to imagine what using a biometric reader would be like. While an attempt was made to mitigate the lack of exposure to biometric hardware by giving a very simplistic description of how the technology would work, one wonders what impact the intangibility of the situation may have had upon the answers given. Secondly, the Canadian banking market is dominated by five banks which may not be the case in other countries. For example, while there are some very large banks in the United States, there are also a variety of relatively smaller banks that may nonetheless still be significant in

terms of their influence, not to mention the variety of regional financial institutions. Therefore, the results obtained in this study may be substantially different from those obtained in countries with a different banking environment. Thirdly, the influence of culture cannot be properly assessed. Although cultural affiliation could have been captured in the survey, various confounding factors (i.e. length of time in Canada, whether they are a new immigrant or second generation immigrant, etc.), combined with the survey size, would have hampered the ability to properly interpret the results.

Third, this study used fingerprints as the method of identity authentication. Given their association with the criminal element, this biometric may make consumers feel they are being equated with criminals which might have impacted their responses to the survey. This may be especially relevant in the minds of consumers if they are aware of the fact that when criminals' fingerprints are processed the *actual* fingerprint is stored in the database as opposed to a mathematical expression. Although the wording in the scenarios tried to compensate for this possibility, there is no guarantee that it would have completely mitigated any misconceptions. While there is the potential that any biometric could result in similar misgivings (e.g. people may worry about the long term medical implications of iris and retinal scans), the perceived stigma associated with fingerprints and criminals may be much more pervasive.

Fourth, this study focused on the Canadian banking industry. As such, its generalisability to other applications is limited. Nonetheless, the model and some of its findings provide direction for further research in different applications, and may even inform practitioners as to appropriate strategies in rolling out biometrics. For example, if an employer is contemplating using biometrics to maintain more accurate time and attendance records for employees, enrolment is probably going to be mandatory. Given the findings of this research, perhaps having shared control (i.e. also requiring a smart card) may mitigate some of the reticence the company may experience from its employees.

Fifth, this research examined attitude as opposed to actual behaviour. However, various studies provide support for the notion that consumer attitude is a strong indicator of actual behaviour (Hassanein and Head 2007; Pavlou and Fygenson 2006; van der Heijden 2003). In addition, given the nature of the technology being investigated, it would be very hard to gauge intention as most people in Canada have not been exposed to biometrics. This inability to draw upon actually experiencing this type of cutting edge technology that may be perceived as too personal and/or intrusive makes truly assessing intention somewhat difficult. Therefore, as people form attitudes about technology that will ultimately influence whether or not they intend to use it, using attitude seemed to be the logical first step when looking at consumer acceptance. Once people become more exposed to biometrics and/or a laboratory experiment can be carried out whereby people can actually experiment with the technology, then it would make more sense to gauge intention.

6.6 Future Research

The empirical results represent an important first step in understanding consumers' attitudes towards using biometrics as a means of identity authentication at ATMs. However, as with most research, the findings suggest a variety of additional directions that should be considered.

While the concept of usefulness, and the survey items used, was adapted from Davis (1989), given the results of the qualitative questions, perhaps there are more dimensions of "usefulness" that need to be explored. Perhaps it is an issue of examining benefits, such as convenience and security. Zhang et al. (2006) propose that convenience is a construct separate from usefulness. In addition, Petter et al. (2007) suggest that usefulness has a multidimensional nature to it with different aspects becoming more or less important depending upon application saying, in essence, that it is a combined reflective and formative construct. These points should be considered in examining the acceptability of biometrics since, given the results from this research, there may be credence to the idea that different aspects of usefulness, or lack thereof, may be weighted differently in the minds of consumers depending upon varying contexts such as control, interoperability, etc. This is discussed further in the following paragraphs.

While consumers appear to understand the value of using biometrics for identity authentication at their banks, what should be explored is whether or not the positive effect of usefulness upon attitude outweighs the negative effect of privacy and security concerns. It would be interesting to determine at what point these two conflicting concepts balance out in the minds of consumers, a "tipping point" if you will, such that the consumer is ambivalent towards the use of biometrics. As it is unlikely that this balance would remain static across applications, the impact of various scenarios and contexts should be examined. However, this would merely be a starting point.

Based upon the results obtained from running PLS, ANOVAs, and examining the responses to the open-ended questions, it would appear that the consumer is simultaneously evaluating a myriad array of conflicting factors when determining the value of biometric authentication. Looking at control for example, as consumer control increases, so does their attitude towards using biometrics. In addition, their privacy and security concerns drop; but so does usefulness. In other words, increased control would appear to make consumers feel better about the prospect of biometrics, presumably due in part to the reduced privacy and security concerns; but this is being mitigated by the loss of convenience associated with now being required to carry a card as with the present debit card system, albeit the latter requires a PIN, which can be forgotten. Furthermore, based upon the initial qualitative study and subsequently demonstrated in the answers to the open ended questions in the final survey, consumers simultaneously see security as a concern and an advantage; and, in conditions of shared control, this advantage is seen as greater, and the concern less, than in the context of bank control. Simply put, when looking at biometrics, the drivers that shape one's attitude appear to be much more complex and seemingly paradoxical than the simple two dimensional concepts, such as

the "privacy/personalization paradox", previously discussed. As such, more qualitative research and focus groups should be employed to further explore some of these simultaneously evaluated contradictory drivers. Such research will hopefully uncover some of the more salient antecedents, as well as contextual settings, enabling the proposed model to be further refined. The usefulness of these approaches would be further enhanced by respondents being able to experiment with the technology as previous research has demonstrated the positive impact of actually experiencing biometrics in a "real" setting (Eschenburg et al. 2005).

The nature of some of the comments made in the open-ended questions suggests that Canadians may not have the background or knowledge with respect to how biometrics work and why they can be much more secure than other classical forms of security. As mentioned previously, this underscores the need for public education; but the question remains as to what should be taught and what would be the impact. Presuming that the banks wish to pursue using biometrics for identity authentication, it would be useful to measure people's initial understanding of biometrics generally and under the proposed context, provide some education through various forums and media, and then measure people's subsequent understanding. This would allow the banks to assess the impact of various educational alternatives which should consequently lead to a better allocation of scarce marketing resources and, hopefully, to a more positive attitude with respect to the use of biometrics in the Canadian banking industry.

Institutional trust was found to influence attitude both directly and indirectly. While the direct impact of institutional trust on attitude was significant ($p < 0.05$), it appears to have a more indirect influence through privacy and security concerns. This mediation effect should be examined further in future research, under varying scenarios and contexts.

This research reaffirmed the importance of control in the minds of consumers when considering initiatives that are perceived as having privacy implications. Recall that it was demonstrated that control was significant when enrolment in the biometric identity authentication program was mandatory, but was not significant when the program was voluntary. It was suggested that this may be due to the supposition by consumers that a voluntary program gives the consumer de facto control in the sense that they don't have to enrol in the first place. Further investigation is needed to fully understand this phenomenon as examining the interaction of control and voluntariness could provide for some interesting future research that could offer practitioners valuable insights as to what the most effective strategies might be when deploying biometric identity authentication technologies.

The previous paragraphs suggest future research along the lines of how to expand upon the concepts and constructs in the proposed model. However, a variety of other avenues for continuing research exist beyond the model. First, as alluded to in the limitations section, only fingerprints were examined in this research. While this

biometric does enjoy a significant market share, face recognition and iris recognition are also quite popular. Also, as face recognition becomes more accurate it will probably attract more of the market. Looking at iris recognition, this is considered to be the most reliable biometric available. However, the costs of the scanners make it prohibitively expensive for widespread use at the present time; but as the costs come down, it may replace fingerprints as the market leader. Then there are the emerging biometrics. This suggests that similar research is required to assess consumer perceptions of acceptability of alternative biometrics.

This research examined consumer acceptability within the financial sector. Given the interests of governments with respect to biometrically enabled documents and of businesses regarding more accurate time and attendance, to name just two potential markets, further research could examine acceptability across a variety of potential applications.

Recall from the qualitative research done with bank personnel that a number of different contexts were identified as being worthwhile to investigate, and this was strictly within the realm of the Canadian banking industry. There are probably a considerable number of contexts of interest to a variety of organizations. These contexts could be examined individually, or in conjunction with other circumstances, to assess how they interact with one another.

Finally, the role of culture cannot be overlooked. While there have been consumer studies done in Europe to assess how different countries feel about potential commercial applications of biometrics, none have examined the antecedents to consumer acceptability. Introducing the element of culture, using the dimensions identified by either Hofstede (2001) or the GLOBE study (House et al. 2004), to assess its impact would be extremely worthwhile from both an academic and practitioner perspective.

While a search of popular media did not reveal any information regarding practitioner research, what was notable was the exhaustive number of recent articles discussing the ongoing global deployment of biometric identity authentication systems across a plethora of applications in both the public and private sectors (see Table 1-1). What is also notable is the backlash this appears to be creating amongst those that are being "forcibly" enrolled without any prior consultation or education. Given these unfortunate circumstances, it is hoped that the research presented in this dissertation is but a first step towards understanding why individuals will, or will not, accept biometric authentication technology thereby establishing some common ground and consensus between those that wish to deploy biometrics, and those upon whom it is deployed.

References

Acquisti, A. and Grossklags, J. "Privacy and Rationality in Individual Decision Making" *IEEE Security & Privacy* January/February, (2005): 26-32.

Adams, A. and Sasse, M. "Users Are Not the Enemy" *Communications of the ACM* 42, no.12, (1999): 41-46.

Adomavicius, G. and Tuzhilin, A. "Personalization Technologies: A Process-Oriented Perspective" *Communications of the ACM* 48, no. 10, (2005): 83-90.

Agarwal, R. and Prasad, J. "A Conceptual and Operational Definition of Personal Innovativeness in the Domain of Information Technology" *Information Systems Research* 9, no. 2, (1998): 204-215.

Ajzen, I. "From Intentions to Actions: A Theory of Planned Behavior" In *Action-Control: From Cognition to Behavior* Ed. J. Kuhl and J. Beckman, New York, NY: Springer-Verlag, (1985): 11-39.

Ajzen, I. "The Theory of Planned Behavior" *Organizational Behavior and Human Decision Processes* 50, no. 2, (1991): 179-211.

Ajzen, I. and Fishbein, M. *Understanding Attitudes and Predicting Social Behavior* (1980): Englewood Cliffs, NJ: Prentice-Hall.

Anderson, J.C. and Gerbing, D.W. "Structural equation Modeling in Practice: A Review and Recommended Two-Step Approach" *Psychological Bulletin* 103, no.3, (1988): 411-423.

Andrews, D.W.K. and Buchinsky, M. "Three-Step Method for Choosing the Number of Bootstrap Repetitions" *Econometrica* 68, no. 1, (2000): 23-51.

Anonymous, "French Authorities Give Sole Approval to GMAT Exam to Collect Biometric Data to Advance Security" (2009), available at: http://pr-usa.net/index.php?option=com_content&task=view&id=237077&Itemid=33

Antony, S., Lin, Z. and Xu, B. "Determinants of Escrow Service Adoption in Consumer-to-Consumer Online Auction Market: An Experimental Study" *Decision Support Systems* 42, no. 3 (2006): 1889-1900.

Avery, R.J. "Determinants of Search for Non-Durable Goods: An Empirical Assessment of the Economics of Information Theory" *The Journal of Consumer Affairs* 30, no. 2, (1996): 390-406.

Awad, N.F. and Krishnan, M.S. "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization" *MIS Quarterly* 30, no. 1, (2006): 13-28.

Ba, S. and Pavlou, P.A. "Evidence of the effect of trust in Electronic Markets: Price Premiums and Buyer Behavior" *MIS Quarterly* 26, no. 3, (2002): 243-266.

Bagozzi, R. P. "Structural Equation Models in Experimental Research" *Journal of Marketing Research* 14, no. 2, (1977): 209-226.

Bagozzi, R.P., Lee, K.H. and Van Loo, M.F. "Decisions to Donate Bone Marrow: The Role of Attitudes and Subjective Norms Across Cultures" *Psychology and Health* 16, no. 1, (2001): 29-56.

Bailey, J.E. and Pearson, S.W. "Development of a Tool for Measuring and Analyzing Computer User Satisfaction" *Management Science* 29, no.5, (1983): 530-545.

Baird, I.S., and Thomas, H. "Toward a Contingency Model of Strategic Risk Taking" *Academy of Management Review* 10, (1985): 230-243.

Bala, D. "Biometrics and Information Security" Proceedings of the *5th Annual Conference on Information Security Curriculum Development (InfoSecCD)* Kennesaw, GA, September (2008): 64-66.

Baldwin, R.L., Green, J.W., Shaw, J.L., and Simpson, D.D. "Physician Risk Attitudes and Hospitalization of Infants with Bronchiolitis" *Academic Emergency Medicine* 12, no. 2, (2005): 142-146.

Barczak, G., Ellen, P.S., and Pilling, B.K. "Developing Typologies of Consumer Motives for Use of Technologically Based Banking Services" *Journal of Business Research* 38, (1997): 131-139.

Bart, Y., Shankar, V., Sultan, F., and Urban, G.L. "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* 69, (2005): 133-152.

Batsell, R.R., and Lodish, L.M. "A Model and Measurement Methodology for Predicting Individual Consumer Choice" *Journal of Marketing Research* 18, (1981): 1-12.

Basole, R.C. "The Value and Impact of Mobile Information and Communication Technologies" *IFAC*, (2004), available at: http://www.ti.gatech.edu/docs/BasoleIFAC2004MobileEnterprises.pdf

Bauer, R.A. "Consumer Behavior as Risk Taking" In *Risk Taking and Information Handling in Consumer Behavior* Ed. D.F. Cox, Cambridge, MA: Harvard University Press, (1967): 389-398.

Belk, R.W. "An Exploratory Assessment of Situational Effects in Buying Behaviour" *Journal of Marketing Research* XI, (May 1974): 156-163.

Belk, R.W. "Situational Variables and Consumer Behaviour" *Journal of Consumer Research* 2, (1975): 157-164.

Bernadette, S. "Empirical Evaluation of the Revised Technology Acceptance Model" *Management Science* 42, no. 1, (1996): 85-93.

Berry, L.L., Seiders, K., and Grewal, D. "Understanding Service Convenience" *Journal of Marketing* 66, no. 3, (2002): 1-17.

Bettman, J.R. "Perceived Risks and Its Components: A Model and Empirical Test" *Journal of Marketing Research* 10 (1973): 184-190.

Bhatnagar, A., Misra, S., and Rao, R. "On Risk, Convenience, and Internet Shopping Behaviour" *Association for Computing Machinery: Communications of the ACM* 43, no. 11, (2000): 98-106.

Bhimani, A. "Securing the Commercial Internet" *Communications of the ACM* 39, no. 6 (1996): 29-35.

Bhide, A. and Stevenson, H. "Trust, Uncertainty, and Profit" *Journal of Socio-Economics* 21, (1992): 191-208.

Bolle, R.M., Connell, J.H., Pankanti, S., Ratha, N.K., and Senior, A.W. *Guide To Biometrics*, New York, NY: Springer Verlag (2004).

Bollen, K.A. *Structural Equations with Latent Variables,* New York, NY: John Wiley and Sons (1989).

Boon, S.D. and Holmes, J.G. "The Dynamics of Interpersonal Trust: Resolving Uncertainty in the Face of Risk" In *Cooperation and Pro-Social Behaviour* Ed. R.H. Hinde and J. Groebel, Cambridge, UK: Cambridge University Press (1991): 190-211.

Boudreau, M.-C., Gefen, D., and Straub, D. "Validation in Information Systems Research: A State-of-the-Art Assessment" *MIS Quarterly* 25, no. 1, (2001): 1-16.

Boukhonine, S., Krotov, V., and Rupert, B. "Future Security Approaches and Biometrics" *Communications of the Association for Information Systems* 16, (2005): 937-966.

Bria, A., Gessler, F., Queseth, O., Stridh, R., Unbehaun, M., Wu, J., and Zander, J. "4th-Generation Wireless Infrastructures: Scenarios and Research Challenges" *IEEE Personal Communications* December (2001): 25-31.

Brinberg, D. and Durnad, J. "Eating at Fast-Food Restaurants – An Analysis Using Two Behavioural Intention Models" *Journal of Applied Social Psychology* 13, no. 6, (1983): 459-472.

Brockhaus, S.R., Sr. "Risk Taking Propensity of Entrepreneurs" *Academy of Management Journal* 23, (1980): 509-520.

Büttner, O.B. and Göritz, A.S. "Perceived Trustworthiness of Online Shops" *Journal of Consumer Behaviour* 7, (2008): 35-50.

Canadian Border Services Agency. "NEXUS", available at: http://www.cbsa-asfc.gc.ca/prog/nexus/menu-eng.html.

Caudill, E., and Murphy, P. "Consumer Online Privacy: Legal and Ethical Issues" *Journal of Public Policy and Marketing* 19, (2000): 7-19.

Chan, P.S. and Pollard, D. "Succeeding in the Dotcom Economy: Challenges for Brick and Mortar Companies" *International Journal of Management* 20, no. 1, (2003): 11-16.

Chang, M.K. "Predicting Unethical Behaviour: A Comparison of the Theory of Reasoned Action and the Theory of Planned Behaviour" *Journal of Business Ethics* 17, no. 16, (1998): 1825-1834.

Chellappa, R.K. and Sin, R.G. "Personalization Versus Privacy: An Empirical Examination of the Online Consumer's Dilemma" *Information Technology and Management* 6, (2005): 181-202.

Chen, Y.-H. and Barnes, S. "Initial Trust and Online Buyer Behaviour" *Industrial Management and Data Systems* 107, no. 1, (2007): 21-36.

Chen, C.-D., Fan, Y.-W. and Farn, C.K. "Predicting Electronic Toll Collection Service Adoption: An Integration of the Technology Acceptance Model and the Theory of Planned Behavior" *Transportation Research Part C* 15, (2007): 300-311.

Chen, R. and He, F. "Examination of Brand Knowledge, Perceived Risk, and Consumers' Intention to Adopt and Online Retailer" *TQM and Business Excellence* 14, no. 6, (2003): 677-693.

Cheong, J.H., and Park, M.-C. "Mobile Internet Acceptance in Korea" *Internet Research* 15, no. 2, (2005): 125-10.

Cheung, C.M.K., Chan, G.W.W. and Limayem, M. "A Critical Review of Online Consumer Behaviour: Empirical Research" *Journal of Electronic Commerce in Organizations* 3, no. 4, (2005): 1-19.

Cheung, C.M.K. and Lee, M.K.O. "Trust in Internet Shopping: Instrument Development and Validation Through Classical and Modern Approaches" *Journal of Global Information Management* 9, no. 3, (2001): 23-35.

Chin, W.W. "Commentary: Issues and Opinion on Structural Equation Modeling" *MIS Quarterly* 22, no. 1, (1998): vii-xvi.

Chin, W.W., Marcolin, B.L. and Newsted, P.R. "A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic-Mail Emotion/Adoption Study" *Information Systems Research* 14, no. 2, (2003): 189-217.

Chin, W.W. and Todd, P.A. "On the Use, Usefulness, and Ease-of-Use of Structural Equation Modeling in MIS Research: A Note of Caution" *MIS Quarterly* 19, no. 2, (1995): 237-246.

Cho, J. and Lee, J. "An Integrated Model of Risk and Risk-Reducing Strategies" *Journal of Business Research* 59, (2006): 112-120.

Chu, P.Y. and Chiu, J.F. "Factors Influencing Household Waste Recycling Behavior: Test of an Integrated Model" *Journal of Applied Social Psychology* 33, no. 3, (2003): 604-626.

Churchill, G.A. "A Paradigm for Developing Better Measures of Marketing Contsructs" *Journal of Marketing Research* 16, no. 1, (1979): 64-73.

CIFAS Online, "Identity Fraud: How Serious is the Problem?", available at: http://www.cifas.org.uk/identity_fraud_is_theft_serious.asp.

Clarke, R. "Human Identification in Information Systems: Management Challenges and Public Policy Issues" *Information Technology and People* 7, no. 4, (1994): 6-37.

Clarke, R. "Internet Privacy Concerns Confirm the Case for Intervention" *Communications of the ACM* 42, (1999): 60-67.

Cockburn, C. and Wilson, T.D. "Business Use of the World Wide Web" *International Journal of Information Management* 16, no. 2 (1996): 83-102.

Cohen, J. *Statistical Power Analysis for the Behavioral Sciences* 2nd Ed. Hillsdale, NJ: Lawrence Erlbaum Associates (1988).

Conchar, M.P., Zinkhan, G.N., Peters, C. and Olavarrieta, S. "An Integrated Framework for the Conceptualization of Consumers' Perceived-Risk Processing" *Journal of the Academy of Marketing Science* 32, no. 4 (2004): 418-436.

Collins, T. "Birmingham Pupils in Protest Over Move to Scan Thumbprints" (2009), available at: http://www.birminghampost.net/news/west-midlands-news/2009/07/13/birmingham-pupils-protest-at-school-s-plan-to-scan-thumbprints-65233-24136556/

Connolly, C. "Performance Testing of Commercial Biometric Systems", *Sensor Review*, 26, no.1, (2006): 33-37.

Corritore, C.L., Kracher, B. and Wiedenbeck, S. "On-line Trust: Concepts, Evolving Themes, a Model" *International Journal of Human-Computer Studies,* no. 58, (2003): 737-758.

Cote, J.A., McCullough, J. and Reilly, M. "Effects of Unexpected Situations on Behaviour-Intention Differences: A Garbology Analysis" *Journal of Consumer Research* 12, (1985): 188-194.

Coventry, L., De Angeli, A. and Johnson, G. "Usability and Biometric Verification at the ATM Interface" Proceedings of the *Special Interest Group on Computer-Human Interaction (SIGCHI) Conference on Human Factors in Computing Systems* Fort Lauderdale, FL, April (2003): 153-160.

Craswell, R. "On the Uses of Trust: Comment on Williamson, 'Calculativeness, Trust, and Economic Organization'" *Journal of Law and Economics* 36, (1993): 487-500.

Cronbach, L.J. "Test Validation" in *Educational Research* (Second Ed.) Ed. R.L. Thorndike, Washington, DC: American Council on Education, (1971): 443-507.

Cuganesan, S. and Lacey, D. "Identity Fraud in Australia: An Evaluation of Its Nature, Cost, and Extent" *Securities Industry Research Centre of Asia-Pacific (SIRCA)* Sydney, Australia, (2003): 1-126.

Culnan, M.J. ""How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use" *MIS Quarterly* 17, no.3, (1993): 341-361.

Culnan, M.J. "Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing" *Journal of Direct Marketing* 9, (1995): 10-19.

Culnan, M.J. "Protecting Privacy Online: Is Self-Regulation Working?" *Journal of Public Policy and Marketing* 19, no. 1, (2000): 20-26.

Culnan, M.J. and Armstrong, P.K. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation" *Organization Science* 10, no. 1, (1999): 104-115.

Culnan, M.J. and Bies, R. "Consumer Privacy: Balancing Economic and Justice Considerations" *Journal of Social Issues* 59, no. 2, (2003): 323-342.

Cunningham, L.F., Gerlach, J. and Harper, M.D. "Perceived Risk and E-Banking Services: An Analysis from the Perspective of the Consumer" *Journal of Financial Services Marketing* 10, no. 2 (2005): 165-178.

Currall, S.C. and Judge, T.A. "Measuring Trust Between Organizational Boundary Role Persons" *Organizational Behavior and Human Decision Processes* 64, (1995): 151-170.

D'Hertefelt, S. *Trust and the Perception of Security*, (2000), available at: http://www.interactionarchitect.com/research/report20000103shd.htm

Das, T.K. and Teng, B.-S. "The Risk-Based View of Trust: A Conceptual Framework" *Journal of Business and Psychology* 19, no. 1 (2004): 85-116.

Das, T.K. and Teng, B.-S. "Time and Entrepreneurial Risk Behavior" *Entrepreneurship Theory and Practice* 22, no. 2 (1997): 69-88.

Davis, F.D. "Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology" *MIS Quarterly* 13, no. 3, (1989): 319-339.

Davis, F.D., Bagozzi, R. and Warshaw, P.R. "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models" *Management Science* 35, no. 8, (1989): 982-1003.

Diamantopoulos, A., and Siguaw, J.A. "Formative Versus Reflective Indicators in Organizational Measure Development: A Comparison and Empirical Illustration" *British Journal of Management* 17, (2006): 263-282.

Diamantopoulos, A., and Winklhofer, H.M. "Index Constructive with Formative Indicators: An Alternative to Scale Development" *Journal of Marketing Research* 38, no. 2, (2001): 269-277.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I. and Colautti, C. "Privacy Calculus Model in E-commerce – A Study of Italy and the United States" *European Journal of Information Systems* 15, (2006): 389-402.

Dinev, T. and Hart, P. "An Extended Privacy Calculus Model for E-commerce Transactions" *Information Systems Research* 17, no. 1 (2006): 61-80.

Dinev, T. and Hart, P. "Internet Privacy Concerns and Their Antecedents – Measurement Validity and Regression Model" *Behaviour and Information Technology* 23, no. 6, (2004): 413-422.

Doney, P.M. and Cannon, J.P. "An Examination of the Nature of Trust in Buyer-Seller Relationships" *Journal of Marketing* 61, no. 2 (1997): 35-51.

Dowling, G.R. "Perceived Risk: The Concept and Its Measurement" *Psychology and Marketing* 3, no. 3 (1986): 193-210.

Dowling, G.R. and Staelin, R. "A Model of Perceived Risk and Intended Risk Handling Activity" *Journal of Consumer Research* 21, no. 1, (1994): 119-154.

Drennan, J., Mort, G.S. and Previte, J. "Privacy, Risk Perception, and Expert Online Behaviour: An Exploratory Study of Household End Users" *Journal of Organizational and End User Computing* 18, no. 1, (2006): 1-22.

Du, Y.E. "Review of Iris Recognition: Camera, Systems, and their Applications" *Sensor Review* 26, no. 1, (2006): 66-69.

Eastlick, M.A. and Feinberg, R. "Shopping Motives for Mail Catalog Shopping." *Journal of Business Research* 45, (1999): 281-290.

Eastlick, M.A. and Lotz, S.L. "Profiling Potential Adopters and Non-Adopters of an Interactive Electronic Shopping Medium" *International Journal of Retail and Distribution Management* 27, no. 6, (1999): 209-223.

Eastlick, M.A., Lotz, S.L. and Warrington, P. "Understanding Online B-to-C Relationships: An Integrated Model of Privacy Concerns, Trust, and Commitment" *Journal of Business Research* 59, (2006): 877-886.

Efron, B. "The Bootstrap and Modern Statistics" *Journal of the American Statistical Association* 95, no. 452, (2000): 1293-1296.

Efron, B. and Tibshirani, R.J. *An Introduction to the Bootstrap (Monographs on Statistics and Applied Probability* New York, NY: Chapman and Hall (1993).

Elliott, A. "Bankers Need to Maintain Vigilance to Eliminate Identity Theft" *Michigan Banker* 19, no. 6, (2007): 70-71.

Elliot, S. and Powell, S. "Expectations Versus Reality: A Snapshot of Consumer Experiences with Internet Retailing." *International Journal of Information Management* 20, (2000): 323-336.

Erickson, R.V. and Haggerty, K.D. *Policing the Risk Society*, University of Toronto Press: Toronto, (1997).

Erlandson, D. A., Harris, E.L., Skipper, B.L. and Allen, S.D. *Doing Naturalistic Inquiry: A Guide to Methods,* Sage Publications (1993).

European Commission *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing or Personal Data and the Protection of Privacy I the Electronic Communications Sector*, European Commission, (2002).

Eschenburg, F., Lylykangas, J., Kramer, N., Surakka, V., Troitzsch, H., Vuorinen, K. and Bente, G. "User Acceptance: The BioSec Approach" *Biometric Technology Today* 13, no. 7, (2005): 8-10.

Featherman, M.S. and Pavlou, P.A. "Predicting e-Services Adoption: A Perceived Risk Facets Perspective" *International Journal of Human-Computer Studies* 59, (2003): 451-474.

Featherman, M.S., Valacich, J.S. and Wells, J.D. "Is That Authentic or Artificial? Understanding Consumer Perceptions of Risk in E-service Encounters" *Information Systems Journal* 16, (2006): 107-134.

Federal Trade Commission (FTC), (2000), available at: http://www.ftc.gov.libaccess.lib.mcmaster.ca/reports/privacy2000/privacy2000.pdf

Federal Trade Commission (FTC), *Curbing Identity Theft*, Federal Trade Commission, Washington, DC, (2003).

Federal Trade Commission (FTC), *Identify Theft Statistics*, Federal Trade Commission, Washington, DC, (2005).

Figge, S. "Situation-Dependent Services – A Challenge for Mobile Network Operators" *Journal of Business Research* 57, (2004): 1416-1422.

Fishbein, M. and Ajzen, I. *Belief, Attitude, Intention, and Behaviour: An Introduction to Theory and Research* Addison-Wesley, Reading, MA, (1975).

Flavián, C. and Guinalíu, M. "Consumer Trust, Perceived Security and Privacy Policy: Three Basic Elements of Loyalty to a Web Site" *Industrial Management and Data Systems* 106, no. 5 (2006): 601-620.

Flynn, L.R. and Goldsmith, R.E. "A Validation of the Goldsmith and Hofacker Innovativeness Scale" *Educational and Psychological Measurement* 53, (1993): 1105-1116.

Fornell, C. and Bookstein, F.L. "Two Structural Equation Models: LISREL and PLS Applied to Consumer Exit-Voice Theory" *Journal of Marketing Research* 19, no. 4, (1982): 440-452.

Fornell, C. and Larcker, D.F. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error" *Journal of Marketing Research* 18, no. 1, (1981a): 39-50.

Fornell, C. and Larcker, D.F. "Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics" *Journal of Marketing Research* 18, no. 3, (1981b): 382-388.

Forsythe, S. and Shi, B. "Consumer Patronage and Risk Perceptions in Internet Shopping" *Journal of Business Research* 56, (2003): 867-875.

Foxman, E. and Kilcoyne, P. "Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issues" *Journal of Public Policy and Marketing* 12, (1993): 106-119.

Fried, C. "Privacy" in F.D. Shoeman (ed.) *Philosophical Dimensions of Privacy* New York: Cambridge Press, (1984).

Fukuyama, F. *Trust: The Social Virtues and the Creation of Prosperity* Free Press: New York, NY (1995).

Galanxhi-Janaqi, H. and Nah, F.F. "U-commerce: Emerging Trends and Research Issues" *Industrial Management and Data Systems* 104, no. 9, (2004): 744-755.

Gambetta, D. *Trust: Making and Breaking Cooperative Relationships* New York, NY: Basil Blackwell Inc. (1990).

Garbarino, E. and Johnson, M. "The Different Roles of Satisfaction, Trust, and Commitment in Customer Relationships." *Journal of Marketing* 63, (1999): 70-87.

Gatignon, H. and Robertson, S. "Innovative Decision Processes" In *Handbook of Consumer Behavior* Ed. T.S. Robertson and H.H. Kassarjian, Englewwod Cliffs, NJ: Prentice-Hall, (1991): 316-348.

Gefen, D. "E-commerce: The Role of Familiarity and Trust." *Omega* 28, no.6 (2000): 725-737.

Gefen, D. "What Makes an ERP Implementation Relationship Worthwhile: Linking Trust Mechanisms and ERP Uselessness" *Journal of Management Information Systems* 21, no. 1, (2004): 262-288.

Gefen, D., Karahanna, E. and Straub, D.W. "Trust and TAM in Online Shopping: An Integrated Model" *MIS Quarterly* 27, no. 1, (2003a): 51-90.

Gefen, D., Karahanna, E. and Straub, D.W. "Inexperience and Experience with Online Stores: The Importance of TAM and Trust" *IEEE Transactions on Engineering Management* 50, no. 3, (2003b): 307-321.

Gefen, D., Rose, G.M., Warkentin, M. and Pavlou, P.A. "Cultural Diversity and Trust in IT Adoption: A Comparison of Potential e-Voters in the USA and South Africa" *Journal of Global Information Management* 13, no. 1, (2005): 54-78.

Gefen, D. and Straub, D.W. "A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example" *Communications of the Association for Information Systems* 16, (2005): 91-109.

Gefen, D. and Straub, D.W. "Managing User Trust in B2C E-Services" *e-Service Journal* 2, no. 2, (2003): 7-24.

Gefen, D., Straub, D.W. and Boudreau, M.-C. "Structural Equation Modeling Techniques and Regression: Guidelines for Research Practice" *Communications of the Association for Information Systems* 4, (2000): 1-78.

Gehrt, K. C. and Yan, R.-N. "Situational, Consumer, and Retailer factors Affecting Internet, Catalogue, and Store Shopping" *International Journal of Retail and Distribution Management* 32, no. 1, (2004): 5-18.

Gerbing, D.W. and Anderson, J.C. "An Updated Paradigm for Scale Development Incorporating Unidimensionality and Its Assessment" *Journal of Marketing Research* 25, no. 2, (1988): 186-192.

Giles, M., McClenahan, C., Carins, E. and Mallet, J. "An Application of the Theory of Planned Behaviour to Blood Donation: The Importance of Self-Efficacy" *Health Education Research* 19, no.4, (2004): 380-391.

Glazer, R. "Marketing in an Information-Intensive Environment: Strategic Implications of Knowledge as an Asset" *Journal of Marketing* 55, no. 4, (1991): 1-20.

Goldenson, R.M. (Ed.) *Longman Dictionary of Psychology and Psychiatry* New York, NY: Longman (1984).

Gordon, G.R., Willox Jr., N.A., Rebovich, D.J., Regan, T.M. and Gordon, J.B. "Identity Fraud: A Critical National and Global Threat", *Journal of Economic Crime Management,* 2, no.1, (2004): 1-48.

Grabner-Kraeuter, S. "The Role of Consumers' Trust in Online Shopping" *Journal of Business Ethics* 39, (2002): 43-50.

Grabner-Kraeuter, S. and Kaluscha, E.A. "Empirical Research in On-Line Trust: A Review and Critical Assessment" *International Journal of Human-Computer Studies* 58, (2003): 783-812.

Granovetter, M.S. "Economic Action and Social Structure" *American Journal of Sociology* 91, (1985): 481-510.

Green, H. "A Little Privacy Please" *BusinessWeek*, March 16, (1998): 98-102.

Green, H. and Hof, R.D. "Lessons of Cyber Survivors" *Business Week* April 22, no. 3779, (2002): 42.

Grewal, D., Gotlieb, J. and Marmorstein, H. "The Moderating Effects of Message Framing and Source Credibility on the Price-Perceived Risk Relationship" *Journal of Consumer Research* 21, no. 1 (1994): 145-153.

Grewal, D., Marmorstein, H. and Sharma, A. "Communicating Price Information Trough Semantic Cues: The Moderating Effects of Situation and Discount Size" *Journal of Consumer Research* 23, (1996): 148-155.

Grijpink, J. "Privacy Law: Biometrics and Privacy." *Computer Law and Security Report* 17, no. 3 (2001): 154-160.

Gronroos, C. "Relationship Approach to Marketing in Service Contexts: The Marketing and Organizational Behaviour Interface." *Journal of Business Research* 20, (1990): 3-11.

Hair, J.F., Anderson, R.E., Tatham, R.L. and Black, W.C. *Multivariate Data Analysis with Readings* 4th Ed. Englewood Cliffs, NJ: Prentice-Hall, (1995).

Hampton-Sosa, W. and Koufaris, M. "The Effect of Website Perceptions on Initial Trust in the Owner Company" *International Journal of Electronic Commerce* 10, no. 1, (2005): 55-81.

Hardgrave, B.C. and Johnson, R.A. "Toward an Information Systems Development Acceptance Model: The Case of Object-Oriented Systems Development" *IEEE Transactions on Engineering Management* 50, no. 3, (2003): 322-336.

Harman, H.H. *Modern Factor Analysis,* (2nd Edition), (1967): Chicago, IL: University of Chicago Press.

Hassanein, K. and Head, M. "Manipulating Perceived Social Presence Through the Web Interface and Its Impact on Attitude Towards Online Shopping" *International Journal of Human-Computer Studies* 65, (2007): 689-708.

Heracleous, L. and Wirtz, J. "Biometrics: The Next Frontier in Service Excellence, Productivity, and Security in the Services Sector", *Managing Service Quality,* 16, no.1, (2006): 12-22.

Hilgard, E., Atkinson, R. and Atkinson, R. *Introduction to Psychology* 6th Ed. New York, NY: Harcourt Brace Jovanovich, (1975).

Hirschman, E.C. "Innovativeness, Novelty Seeking, and Consumer Creativity" *Journal of Consumer Research* 7, no. 3, (1980): 283-295.

Hirunyawipada, T. and Paswan, A.K. "Consumer Innovativeness and Perceived Risk: Implications for High Technology Product Adoption" *Journal of Consumer Marketing* 23, no.4, (2006): 182-198.

Hitt, M.A. and Tyler, B.B. "Strategic Decision Models: Integrating Different Perspectives" *Strategic Management Journal* 12, (1991): 327-351.

Hocutt, M. "Relationship Dissolution Model: Antecedents of Relationship Commitment and the Likelihood of Dissolving a Relationship." *International Journal of Service Industry Management* 9, no. 2 (1998):189-200.

Hoffman, D., Novak, T. and Peralta, M. "Building Consumer Trust Online" *Communications of the ACM* 42, (1998): 80-85.

Hofstede, G.H. *Culture's Consequences,* (2nd Edition), (2001): Beverly Hills, CA: Sage Publications.

Holtfreter, R.A. and Holtfreter, K. "Gauging the Effectiveness of US Identity Theft Legislation" *Journal of Financial Crime* 13, no. 1, (2006): 56-64.

Hopkins, H. "An Introduction to Biometrics and Large Scale Civilian Identification", *International Review of Law, Computers, and Technology* 13, no. 3, (1999): 337-363.

House, R.J., Hanges, P.J., Javidan, M., Dorfman, P.W. and Gupta, V. *Culture, Leadership, and Organizations: The GLOBE Study of 62 Societies* (2004): Thousand Oaks, CA: Sage Publications.

Hsu, C.L. and Lu, H.P. "Why Do people Play On-line Games? An Extended TAM with Social Influences and Flow Experience" *Information and Management* 41, no. 7, (2004): 853-868.

Hsu, S.-H., Chen, W.-H. and Hsieh, M.-J. "Robustness Testing of PLS, LISREL, EQS, and ANN-based SEM for Measuring Customer Satisfaction" *Total Quality Management* 17, no. 3, (2006): 355-371.

Hulland, J. "Use of Partial Least Squares (PLS) in Strategic Management Research: A Review of Four Recent Studies" *Strategic Management Journal* 20, no. 2, (1999): 195-203

Ingene, C.A. and Hughes, M.A. "Risk Management by Consumers" In *Research in Consumer Behaviour* Vol. 1 Ed. J. Sheth, Greenwich, CT: JAI, (1985): 103-158.

International Biometric Group (IBG), "Biometrics Market and Industry Report 2009-2014" (2009a), available at: http://www.biometricgroup.com/reports/public/market_report.php

International Biometric Group (IBG), "How Do Biometric Systems Determine Matches?" (2009b), available at: www.biometricgroup.com/reports/public/reports/biometric_match.html

Jacoby, J. and Kaplan, L. "The Components of Perceived Risk" *Advances in Consumer Research* 3, (1972): 382-382.

Jackson, B. "Ontario has new method to keep problem gamblers out of gaming sites – your face!" (2009), available at: http://itbusiness.ca/it/client/en/home/News.asp?id=52571

Jain, A.K., Ross, A. and Prabhakar, S. "An Introduction to Biometric Recognition", *IEEE Transactions on Circuits and Systems for Video Technology,* 14, no, 1, (2004): 14-20.

James, T., Pirim, T., Boswell, K., Reithel, B. and Barkhi, R. "Determining the Intention to use Biometric Devices: An Application and extension of the Technology Acceptance Model" *Journal of Organizational and End User Computing* 18, n0. 3, (2006): 1-24.

Jarvenpaa, S. L., Tractinsky, N. and Vitale, M. "Consumer Trust in an Internet Store" *Information Technology and Management* 1, no. 12 (2000): 45-71.

Jarvenpaa, S.L., Tractinsky, N. and Saarinen, L. "Consumer Trust in an Internet Store: A Cross Cultural Validation" *Journal of Computer-Mediated Communication* 5, no. 2, (1999):

Jarvis, C.B., MacKenzie, S.B and Podsakoff, P.M. "A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research" *Journal of Consumer Research* 30, no.2, (2003): 199-218.

Javelin. "2006 Identity Fraud Survey Report" *Javelin Strategy and Research*, (2006), available at: http://www.javelinstrategy.com/uploads/603.R_2006IdentityFraudSurvey.pdf

Javelin. "2007 Identity Fraud Survey Report: Identity Fraud is Dropping, Continued Vigilance is Necessary" *Javelin Strategy and Research*, (2007), available at: http://www.javelinstrategy.com/uploads/701.R_2007IdentityFraudSurveyReport_Brochure.pdf

Johnston-George, C. and Swap, W.C. "Measurement of Specific Interpersonal Trust: Construction and Validation of a Scale to Assess Trust in a Specific Other" *Journal of Personality and Social Psychology* 43, (1982): 1306-1317.

Joines, J.L., Scherer, C.F. and Scheufele, D.D. "Exploring Motivations for Consumer Web Use and their Implications for e-Commerce", *Journal of Consumer Marketing,* 20, no.2/3, (2003): 90-108.

Kaplan, D. *Structural Equation Modeling: Foundations and Extensions* (2000): Thousand Oaks, CA: Sage Publications.

Keppel, G. *Design and Analysis: A Researcher's Handbook.* Prentice-Hall, Englewood Cliffs, NJ, (1991).

Kerlinger, F.N. *Foundations of Behavioural Research* New York: Holt, Rinehart, and Winston.

Kim, H. "Biometrics, Is It a Viable Proposition for Identity Authentication and Access Control?" *Computers and Security* 14, (1995): 205-214.

Kim, D.J., Ferrin, D.L. and Rao, H.R. "A Trust-Based Consumer Decision-Making Model in Electronic Commerce: The Role of Trust, Perceived Risk, and Their Antecedents" *Decision Support Systems* 44, (2008): 544-564.

Kimery, K.M. and McCord, M. "Third-Party Assurances: Mapping the Road to Trust in E-tailing" *Journal of Information Technology Theory and Application* 4, no. 2, (2002): 63-82.

Kirton, M. "Adaptors and Innovators: A Description and Measure" *Journal of Applied Psychology* 61, no. 5, (1976): 622-629.

Kitchenham, B. and Pfleeger, S. "Principles of Survey Research Part 4: Questionnaire Evaluation" *Software Engineering Notes* 27, no. 3 (2002): 20-23.

Klaas, B.S. and Wheeler, H.N. "Managerial Decision Making About Employee Discipline: A Policy-Capturing Study" *Personnel Psychology* 43, (1990): 117-133.

Kleist, V.K. "Building Technologically Based Online Trust: Can the Biometrics Industry Deliver the Online Trust Silver Bullet?" *Information Systems Management* 24, no. 4, (2007): 319-329.

Kling, R. and Allen, J.P. "How the Marriage of Management and Computing Intensifies the Struggle for Personal Privacy" In *Computers, Surveillance, and Privacy* Ed. D. Lyon and E. Zureik Minneapolis, MN: University of Minnesota Press, (1996): 104-131.

Költzsch, G. "Innovative Methods to Enhance Transaction Security of Banking Applications" *Journal of Business Economics and Management* 7, no. 4, (2006): 243-249.

Korgaonkar, P. K. and Wolin, L. D. "A Multivariate Analysis of Web Usage" *Journal of Advertising Research* 39, no. 2, (1999): 53-68.

Koufaris, M. "Applying the Technology Acceptance Model and Flow Theory to Online Consumer Behaviour" *Information Systems Research* 13, no. 2, (2002): 205-223.

Koufaris, M. and Hampton-Sosa, W. "The Development of Initial Trust in an Online Company by New Customers" *Information and Management* 41, (2004): 377-397.

Langenderfer, J. and Linnhoff, S. "The Emergence of Biometrics and Its Effect on Consumers" *The Journal of Consumer Affairs* 39, no. 2 (2005): 314-338.

Larsen, T.J. and Sørebø, Ø. "Impact of Personal Innovativeness on the Use of the Internet Among Employees at Work" Journal of Organizational & End User Computing 17, no. 2 (2005): 43-63.

Lassar, W.M., Manolis, C. and Lassar, S.S. "The Relationship Between Consumer Innovativeness, Personal Characteristics, and Online Banking Adoption" *The International Journal of Bank Marketing* 23, (2005): 175-199.

Laufer, R.S. and Wolfe, M. "Privacy as a Concept and a Social Issue: A Multidimensional Development Theory" *Journal of Social Issues* 33, no. 3 (1977): 22-42.

Lease, D.R. "Factors Influencing the Adoption of Biometric Security Technologies by Decision Making Information Technology and Security Managers" Ph.D. Dissertation, Capella University, (2005).

Lee, Y., Kozar, K. and Larsen, L., (2003) "The Technology Acceptance Model: Past, Present, and Future" *Communications of the Association for Information Systems* 12, no. 50, (2003): 752-780.

Lee, M. and Turban, E. "Trust in B-to-C Electronic Commerce: A Proposed Research Model and Its Application" *International Journal of Electronic Commerce* 6. no. 1, (2001): 75-91.

Lee, E.-J. and Overby, J. "Creating Value for Online Shoppers: Implications for Satisfaction and Loyalty." *Journal of Consumer Satisfaction* 17, (2004): 54-68.

Legris, P., Ingham, J. and Collerette, P. "Why Do People Use Information Technology? A Critical Review of the Technology Acceptance Model" *Information and Management* 40, (2003): 191-204.

Lewan, T. "Chips in Official IDs Raise Privacy Fears" (2009), available at: http://www.google.com/hostednews/ap/article/ALeqM5hHq9P54bYfXbHp-aDgs01gePq1twD99CDMT00

Lewicki, R.J. and Bunker, B. "Trust in Relationships: A Model of Trust Development and Decline" in B. Bunker and J. Rubin (eds.), *Conflict, Cooperation, and Justice* (Jossey-Bass, San Francisco), (1995): 133-173.

Liang, H., Saraf, N., Hu, Q. And Xue, Y. "Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management" *MIS Quarterly* 31, no. 1, (2007): 59-87.

Liao, Z. and Cheung, M. "Internet-based e-Shopping and Consumer Attitudes: An Empirical Study" *Information and Management* 38, no. 5, (2001): 299-306.

Liebermann, Y. and Stashevsky, S. "Perceived Risks as Barriers to Internet and E-commerce Usage" *Qualitative Marketing Research: An International Journal* 5, no. 4 (2002): 291-300.

Litan, A. "The Truth Behind identity Theft Numbers" *Gartner, Inc.* (2007).

Liu, C., Marchewka, J.T., Lu, J. and Yu, C.-S. "Beyond Concern: A Privacy-Trust-Behavioural Intention Model of Electronic Commerce" *Information and Management* 42, (2004): 127-142.

López-Nicolás, C. and Molina-Castillo, F.J. "An Assessment of Advanced Mobile Services Acceptance: Contributions from TAM and Diffusion Theory Models" *Information and Management* 45, no. 6 (2008): 359-364.

Malhotra, N.K., Kim, S.S. and Agarwal, J. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model" *Information Systems Research* 15, no. 4, (2004): 336-355.

Malhotra, N.K. *Marketing Research: An Applied Orientation* 4th ed. (2004): Upper Saddle River, NJ: Prentice-Hall.

Martocchio, J. and Judge, T.A. "A Policy-Capturing Approach to Individual's Decisions to be Absent" *Organization Behaviour and Human Decision Processes* 57, (1994): 358-386.

Mason, R. "Four Ethical Issues of the Information Age" *MIS Quarterly* 10, no. 1 (1986): 4-12.

Matyas Jr., V. and Riha, Z. "Biometrics Authentication Systems", Brno, Czech Republic, Faculty of Informatics, Masaryk University. (2000) www.fi.muni.cz/veda/reports/files/oldeer/FIMU-RS-2000-08.pdf

Mathwick, C., Malhouta, N. and Rigdon, E. "The Effect of Dynamic Retail Experiences on Experiential Perceptions of Value: An Internet and Catalog Comparison" *Journal of Retailing* 78, (2002): 51-60.

Mayer, R.C. and Davis, J.H.; Schoorman, F. David. "An Integrative Model of Organizational Trust" *Academy of Management Review* 20, no. 3 (1995): 709-734.

McCloskey, D.W. "The Importance of Ease of Use, Usefulness, and Trust to Online Consumers: An Examination of the Technology Acceptance Model with Older Consumers" *Journal of Organizational and End User Computing* 18, no. 3, (2006): 47-65.

McCrohan, K.F. "Facing the Threats to Electronic Commerce" *Journal of Business and Industrial Marketing* 18, no. 2 (2003): 133-145.

McKnight, D.H., Choudhury, V. and Kacmar, C. "Developing and Validating Trust Measures for E-Commerce: An Integrative Typology" *Information Systems Research* 13, no. 3, (2002a): 334-359.

McKnight, D.H., Choudhury, V. and Kacmar, C. "The Impact of Initial Consumer Trust on Intentions to Transact with a Website: A Trust Building Model" *Journal of Strategic Information Systems* 11, no. 3/4 (2002b): 297-323.

McKnight, D.H., Cummings, L.L. and Chervany, N.L. "Initial Trust Formation in New Organizational Relationships" *Academy of Management Review* 23, no. 3, (1998): 473-490.

Mercuri, R.T. "Scoping Identity Theft" *Communications of the ACM* 49, no. 5, (2006): 17-21.

Meyerson, D., Weick, K.E. and Kraner, R.M. "Swift Trust and Temporary Groups" In *Trust in Organizations: Frontiers of Theory and Research* Ed. R.M. Kramere and T.R. Tyler, Thousand Oaks, CA: Sage Publications, (1996): 166-195.

Midgley, D.F. and Dowling, G.R. "Innovativeness: The Concept and Its Measurement" *Journal of Consumer Research* 4, (1978): 229-242.

Miles, M. B. and Huberman, A. M. *Qualitative Data Analysis: An Expanded Sourcebook.* 2nd edition (1994).

Miller, M. "Biometric Security to Drive $7.3 Billion in Five Years, According to ABI" *Electronic News* 54, no. 30, (2008): 11.

Miller, R. "Global Biometrics Forecast to 2012" (2009), available at: http://www.reportlinker.com/p096440/Global-Biometric-Forecast-to-2012.html?utm_source=LivePR&utm_medium=pr&utm_campaign=LivePR

Milne, G.R. "How Well Do Consumers Protect Themselves from Identity Theft?" *The Journal of Consumer Affairs* 37, no. 2, (2003): 388-402.

Milne, G.R. and Rohm, A. "Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-In and Opt-Out Alternatives" *Journal of Public Policy and Marketing* 19, no. 2 (2000): 238-249.

Milne, G.R.; Culnan, M.J. "Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online privacy Notices" *Journal of Interactive Marketing* 18, no. 3, (2004): 15-29.

Milne, G.R., Rohm, A. and Bahl, S. "Consumers' Protection of Online Privacy and Identity" *The Journal of Consumer Affairs* 38, no. 2 (2004): 217-232.

Mitchell, V.-W. "Consumer Perceived Risk: Conceptualizations and Models" *European Journal of Marketing* 33, no.1/2 (1999): 163-195.

Mitchell, V.-W. and Greatorex, M. "Risk Perception and Reduction in the Purchase of Consumer Services" *Services Industries Journal* 13, (1993): 179-200.

Miyazaki, A. and Fernandez, A. "Internet Privacy and Security: An Examination of Online Retailer Disclosures" *Journal of Public Policy and Marketing* 19, no. 1 (2000): 54-61.

Miyazaki, A. and Fernandez, A. "Consumer Perceptions of Privacy and Security Risks for Online Shopping" *The Journal of Consumer Affairs* 35, no. 1 (2001): 27-44.

Monsuwé, T.P., Dellaert, B.G. and De Ruyter, K. "What Drives Consumers to Shop Online? A Literature Review." *International Journal of Service Industry Management,* 15, no.1, (2004): 102-121.

Moody, J. "Public Perceptions of Biometric Devices: The Effect of Misinformation on Acceptance and Use", http://articles.iisit.org/102moody.pdf (Accessed May, 2006).

Moon, J.-W., and Kim, Y.-G. "Extending the TAM for a World-Wide-Web Context" *Information and Management* 38, (2001): 217-230.

Moore, G.C. and Benbasat, I. "Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation", *Information Systems Research* 2, no. 3, (1991): 192-222.

Morgan, R.M. and Hunt, S.D. "The Commitment-Trust Theory of Relationship Marketing" *Journal of Marketing* 58, no. 3, (1994): 20-38.

Morris, M.G. and Venkatesh, V. "Age Differences in Technology Adoption Decisions: Implications for a Changing Work Force" *Personnel Psychology* 5, no. 2, (2000): 375-403.

Morse, N.J. "Combating Risk Creep" *Mortgage Banking* 66, no. 6, (2006): 137-139.

Most, C.M. "Biometrics and Trusted Identity: Combatting Identity Theft", (2005), available at: www.findbiometrics.com/Pages/feature%20articles/identitytheft.html.

Mukherjee, A and Nath, P. "A Model of Trust in Online Relationship Banking" *International Journal of Bank Marketing* 21, no. 1, (2003): 5-15.

Murthi, B.P.S. and Sarkar, S. "The Role of Management Sciences in Research on Personalization" *Management Science* 49, no. 10, (2003): 1344-1362.

Nunn, S. "How Capital Technologies Affect Municipal Service Outcomes: The Case of Police Mobile Digital Terminals and Stolen Vehicle Recoveries" *Journal of Police Analysis and Management* 13, no. 3, (1994): 539-559.

Nunn, S. "Seeking Tools for the War On Terror" *Policing: An International Journal of Police Strategies and Management* 26, no. 3, (2003): 454-472.

Nunn, S. and Quinet, K. "Evaluating the Effects of Information Technology on Problem-Oriented Policing: If It Doesn't Fit, Must We Quit?" *Evaluation Review* 26, no. 1, (2002).

Nunnally, J.C. *Psychometric Theory* 2nd Ed. New York, NY: McGraw Hill (1978).

O'Cass, A. and Fenech, T. "Webretailing Adoption: Exploring the Nature of Internet Users Web Retailing Behaviour" *Journal of Retailing and Consumer Services* 10, (2003): 81-94.

O'Donoghue, T. and Rabin, M. "The Economics of Immediate Gratification" *Jornal of Behavioural Decision Making* 13, no. 2, (2000): 233-250.

Olivero, N. and Lunt, P. "Privacy Versus Willingness to Disclose in E-commerce Exchanges: The Effect of Risk Awareness on the Relative Role of Trust and Control" *Journal of Economic Psychology* 25, (2004): 243-262.

Orwell, G. *1984.* London: Secker and Warburg (1951).

Pan, Y. and Zinkhan, G.M. "Exploring the Impact of Online Privacy Disclosures on Consumer Trust" *Journal of Retailing* 82, no. 4, (2006): 331-338.

Parasuraman, A. and Zinkham, G. "Marketing To and Serving Customers Through the Internet: An Overview and Research Agenda" *Academy of Marketing Science* 30, no. 4 (2002): 286-296.

Park, C.-H. and Kim, Y.-G. "Identifying Key Factors Affecting Consumer Purchase Behaviour in an Online Shopping Context." *International Journal of Retail and Distribution Management* 31, no.1 (2003): 16-29. 19, no. 1, (2000): 27-41.

Pavlou, P.A. "Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model" *International Journal of Electronic Commerce* 7, no. 3, (2003): 101-134.

Pavlou, P.A. and Gefen, D. "Building Effective Online Marketplaces with Institution-Based Trust" *Information Systems Research* 15, no. 1, (2004): 37-59.

Pavlou, P.A., Liang, H. and Xue, Y. "Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective" *MIS Quarterly* 31, no. 1, (2007): 105-136.

Perakslis, C. and Wolk, R. "Social Acceptance of RFID as a Biometric Security Method" *IEEE Technology and Society Magazine* 25, no. 3, (2006): 34-42.

Petouhoff, N. and Johnson, B. "How Much Is Your Customers' Trust Worth" *Customer Relationship Management* 10, no. 9, (2006): 48.

Perry 6. "Who Wants Privacy Protection and What do They want?" *Journal of Consumer Behaviour* 2, no. 1, (2002): 80-100.

Petter, S., Straub, D.W. and Rai, A. "Specifying Formative Constructs in Information Systems Research" *MIS Quarterly* 31, no. 4, (2007): 623-656.

Pew Internet and America Life Project "Online Banking: A Pew Internet Project Data Memo", available at: http://www.pewinternet.org/pdfs/PIP_Online_Banking.pdf.

Phelps, J., Nowak, G. and Ferrell, E. "Privacy Concerns and Consumer Willingness to Provide Personal Information" *Journal of Public Policy and Marketing*

Piazza, P. "The Smart Cards Are Coming...Really", *Security Management* 49, no.1, (2005): 40-52.

Pikkarainen, T., Pikkarainen, K., Karjaluoto, H. and Pahnila, S. "Consumer Acceptance of Online Banking: An Extension of the Technology Acceptance Model" *Internet Research-Electronic Networking Applications and Policy* 14, no. 3, (2004): 224-235.

Pires, G., Stanton, J. and Eckford, A. "Influences on the Perceived Risk of Purchasing Online" *Journal of Consumer Behaviour* 4, no. 2, (2004): 118-131.

Pirim, T., James, T., Boswell, K., Reithel, B. and Barkhi, R. "An Empirical Investigation of an Individual's Perceived Need for Privacy and Security" *(Working Paper)* Virginia Polytechnic Institute and State University, (2004).

Plouffe, C.R., Hulland, J.S. and Vandenbosch, Mark. "Research Report: Richness Versus Parsimony in Modeling Technology Adoption Decisions – Understanding Merchant Adoption of a Smart Card-Based Payment System" *Information Systems Research* 12, no. 2, (2001): 208-222.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.-Y. and Podsakoff, N.P. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies" *Journal of Applied Psychology* 88, no. 5, (2003): 879-903.

Podsakoff, P.M. and Organ, D.W. "Self-Report in Organizational Research: Problems and Prospects" *Journal of Management* 12, no. 4, (1986): 531-544.

Prabakar, S., Pankatani, S. and Jain, Anil. "Biometric Recognition: Security and Privacy Concerns" *IEEE Security and Privacy* 1, no.2, (2003): 33-42.

Pritchard, M., Havitz, M. and Howard, D. "Analyzing the Commitment-Loyalty Link in Service Contexts." *Journal of the Academy of Management Science* 27, no.3 (1999): 333-348.

Puffer, S. and Rashidian, A. "Practice Nurses' Intentions to Use Clinical Guidelines" *Journal of Advanced Nursing* 47, no. 5, (2004): 500-509.

QSR. "NVivo Qualitative Data Analysis Software" (2008), available at: www.qsrinternational.com

Ramaswamy, V.M. "Identity-Theft Toolkit" *The CPA Journal* 76, no. 10, (2006): 66-70.

Ranganathan, C. and Ganapathy, S. "Key Dimensions of B2C Websites" *Information and Management* 39, (2002): 457-465.

Ranganathan, C. and Grandon, Elizabeth. "An Exploratory Examination of Factors Affecting Online Sales" *The Journal of Computer Information Systems* 42, no. 3, (2002): 87-93.

Reid, P. *Biometrics for Network Security*, Upper Saddle River, N.J., Prentice Hall, (2004).

Remus, W. "Using Students as Subjects in Experiments on Decision Support Systems" *Twenty-Second Hawaii International Conference on Systems Sciences* (1989): 176-180

Resnick, M.L. and Montania, R. "Perceptions of Customer Service, Information Privacy, and Product Quality from Semiotic Design Features in an Online Web Store" *International Journal of Human-Computer Interaction* 16, no. 2, (2003): 211-234.

Retsky, M.L. "Just Posting Cookies Agreement Not Enough" *Marketing News* 35, no. 20, (2000): 12-13.

Ringle, C., Wende, S. and Will, A. *Smart-PLS Version 2.0 M3* (2008), available at: http://www.smartpls.de

Rogers, E.M. *Diffusion of Innovations*, 4th Ed., The Free Press, New York, NY, (1995).

Rotter, J.B. "Generalized Expectancies for Interpersonal Trust" *American Psychologist* 26, (1971): 443-450.

Rousseau, D.M., Sitkin, S.B., Burt, R.S. and Camerer, C. "Not So Different After All: A Cross-Discipline View of Trust" *Academy of Management Review* 23, no. 4: 393-404.

Roussos, G., Koukara, L., Kourouthanasis, P., Tuominen, J., Seppala, O., Giaglis, G. and Jeroen, F. "A Case Study in Pervasive Retail" in M. Viveros and H. Lei (eds.) *ACM MOBICOM Second International Workshop in Mobile Comerce* Atlanta: ACM Press, (2002): 90-94.

Rudall, B.H. "Contemporary Systems and Cybernectics: Biometric Systems", *Kybernetes,* 33, no. 8 (2004): 1235-1243.

Saban, K., McGivern, E., Saykiewicz, J. "A Critical Look at the Impact of Cybercrime on Consumer Internet Behaviour." *Journal of Marketing Theory and Practice* 10, no.2 (2002): 29-37.

Salisbury, W.D., Pearson, R.A., Pearson, A.W. and Miller, D.W. "Perceived Security and World Wide Web Purchase Intention" *Industrial Management and Data Systems* 101, no. 4, (2001):

Schneider, S.L. and Lopes, L.L. "Reflection in Preferences Under Risk: Who and When May Suggest Why" *Journal of Experimental Psychology: Huamn Perception and Performance* 12, (1986): 535-548.

Schurr, P.H. and Ozanne, J.L. "Influences on Exchange Processes: Buyers' Preconceptions of a Seller's Trustworthiness and Bargaining Toughness" *Journal of Consumer Research* 11, no. 4 (1985): 939-953.

Schaupp, L.C. and Bélanger, F. "A Conjoint Analysis of Online Consumer Satisfaction" *Journal of Electronic Commerce Research* 6, no. 2, (2005): 95-111.

Schlenker, B.R., Helm, B. and Tedeschi, J.T. "The Effects of Personality and Situational Variables on Behavioral Trust" *Journal of Personality and Social Psychology* 25, (1973): 419-427.

Segars, A. "Assessing the Unidimensionality of Measurement: A Paradigm and Illustration within the Context of Information Systems" *Omega* 25, no. 1 (1997): 107-121.

Serenko, A. *User Adoption of Interface Agents for Electronic Mail* Ph.D. Thesis, McMaster University, (2005).

Sheehan, K.B. "Toward a Typology of Internet Users and Online Privacy Concerns" *The Information Age* 18, no. 1, (2002): 21-32.

Sheehan, K.B. and Hoy, M.G. "Dimensions of Privacy Concern Among Online Consumers" *Journal of Public Policy and Marketing* 19, no. 1, (2000): 62-73.

Shemwell, D.J., Yavas, U. and Bilgin, Z. "Customer-Service Provider Relationships: An Empirical Test of a Model of Service Quality, Satisfaction, and Relationship-Oriented Outcomes." *Internal Journal of Service Industry Management* 9, no. 2 (1998): 155-168.

Sheng, H., Nah, F.F. and Siau, K. "An Experimental Study on U-commerce Adoption: Impact of Personalization and Privacy Concerns" In *5th Pre-ICIS Annual Workshop on HCI Research in MIS*, Milwaukee, WI (2006): 80-84.

Shih, H.P. "An Empirical Study on Predicting User Acceptance of E-Shopping on the Web" *Information and Management* 41, no. 3, (2004): 351-368.

Shih, Y.-Y. and Fang, K. "Effects of Network Quality Attributes on Customer Adoption Intentions of Internet Banking" *Total Quality Management and Business Excellence* 17, no. 1, (2006): 61-77.

Shu-Fong, L., Yin, F.M., Ming, S.S.K. and Ndubisi, N.O. "Attitude Towards Internet Banking: A Study of Influential factors in Malaysia" *International Journal of Services Technology and Management* 8, no. 1, (2007): 41.

Simon, H.A. *Models of Bounded Rationality*, MIT Press, (1982).

Singh, S. "The Social Dimensions of the Security of Internet Banking" *Journal of Theoretical and Applied Electronic Commerce Research* 1, no. 2, (2006): 72-78.

Siponen, M.T. "A Conceptual Foundation for Organizational Information Security Awareness" *Information Management and Computer Security* 8, no. 1, (2000): 31-41.

Sitkin, S.B. and Roth, N.L. "Explaining the Limited Effectiveness of Legalistic 'Remedies' for Trust/Distrust" *Organizational Science* 4, (1993): 367-392.

Sitkin, S.B. and Weingart, L.R. "Determinants of Risky Decision-Making Behavior: A Test of the Mediating Role of risk Perceptions and Propensity" *Academy of Management Journal* 38, no. 6 (1995): 1573-1592.

Slovic, P. "Psychological Study of Human Judgment: Implications for Investment Decision Making" *Journal of Finance* 27, (1972): 779-799.

Smith, A.D. "Cybercriminal Impacts on Online Business and Consumer Confidence", *Online Information Review,* 28, no.3, (2004): 224-234.

Smith, H.J., Milberg, S.J. and Burke, S.J. "Information Privacy: Measuring Individuals' Concerns about Organizational Practices" *MIS Quarterly*, 20, no.2, (1996): 167-196.

Sproule, S. and Archer, N. "Measuring Identity Theft in Canada: 2008 Consumer Survey" *McMaster e-business Research Centre (MeRC)* no. 23, July (2008): 1-70.

Stevens, J. *Applied Multivariate Statistics for the Social Sciences* 3rd Ed. Mahwah, NJ: Lawrence Erlbaum Associates, Inc. (1996).

Stewart, K.A. and Segars, A.H. "An Empirical Examination of the Concern for Information Privacy Instrument" *Information Systems Research* 13, no. 1, (2002): 36-49.

Straub, D.W. "Validating Instruments in MIS Research" *MIS Quarterly* 13, no. 2, (1989): 147-169.

Straub, D.W. "Effective IS Security: An Empirical Study" *Information Systems Research* 1, no. 2, (1990): 255-277.

Straub, D.W. and Karahanna, E. "Knowledge Worker Communications and Recipient Availability: Toward a Task Closure Explanation of Media Choice" *Organization Science* 9, no. 2, (1998): 160-175.

Straub, D.W., Boudreau, M.-C. and Gefen, D. "Validation Guidelines for IS Positivist Research" *Communications of the Association for Information Systems* 13, (2004): 380-427.

Suh, B. and Han, I. "Effect of Trust on Consumer Acceptance of Internet Banking" *Electronic Commerce Research and Applications* 1, (2002): 247-263.

Sukhai, N.B. "Access Controls and Biometrics" Proceedings of the *1st Annual Conference on Information Security Curriculum Development (InfoSecCD)* Kennesaw, GA, October (2004): 124-127.

Sutherland, S. (Ed.) *International Dictionary of Psychology* New York, NY: Continuum (1989).

Swartz, N. "Data Breaches: Is Anyone Safe?" *Information Management Journal* 39, no. 4, (2005a): 10.

Swartz, N. "Study Reveals Consumers' Data Worries" *Information Management Journal* 39, no. 5, (2005b): 10.

Szymanski, D. and Hise, R. "e-Satisfaction: An Initial Examination." *Journal of Retailing* 76, no.3 (2000): 309-322.

Tan, M. and Teo, T.S.H. "Factors Influencing the Adoption of Internet Banking" *Journal of the Association for Information Systems* 1, (2000): 1-38.

Taylor, S. and Todd, P.A. "Understanding Information Technology Use: A Test of Competing Models" *Information Systems Research* 6, no. 2, (1995): 144-176.

Tenenhaus, M., Vinzi, V.E., Chatelin, Y.-M. and Lauro, C. "PLS Path Modeling" *Computational Statistics and Data Analysis* 48, (2005): 159-205.

Teo, H.H., Wei, K.K. and Benbasat, I. "Predicting Intention to Adopt Interorganizational Linkages: An Institutional Perspective" *MIS Quarterly* 27, no. 1, (2003): 19-49.

Thomas, A. "IBM Inks UK Biometric Passport Deal" (2009), available at: http://www.tgdaily.com/content/view/43186/108/

Torkzadeh, G. and Dhillon, G. "Measuring Factors that Influence the Success of Internet Commerce" *Information Systems Research* 13, no.2 (2002): 187-225.

Torregoza, H.L. "Solons Say 25 M Voters Might Not Be Able to Vote in 2010" (2009), available at: http://mb.com.ph/articles/210417/solons-say-25-m-voters-might-not-be-able-vote-2010

Valcav, M. and Zdenek, R. "Biometric Authentication Systems", Technical Report, (2000), available at: www.ecom-monitor.com/papers/biometricsTR2000.pdf.

van der Heijden, H., Verhagen, T. and Creemers, M. "Understanding Online Purchase Intentions: Contributions from Technology and Trust Perspectives" *European Journal of Information Systems* 12, (2003): 41-48.

Van Dyke, T.P., Midha, V. and Nemati, H. "The Effect of Consumer Privacy Empowerment on Trust and Privacy Concerns in E-Commerce" *Electronic Markets* 17, no. 1, (2007): 68-81.

Venkatesh, V. "Determinants of Perceive Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion Into the Technology Acceptance Model" *Information Systems Research* 11, no. 4, (2000): 342-365.

Venkatesh, V. and Davis, F. "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Studies" *Management Science* 46, no. 2, (2000): 186-204.

Venkatesh, V., Morris, M., Davis, G. and Davis, F. "User Acceptance of Information Technology: Toward a Unified View." *MIS Quarterly* 27, no. 3 (2003): 425-478.

Verhagen, T., Meents, S. and Tan, Y.-H. "Perceived Risk and Trust Associated with Purchasing at Electronic Marketplaces" *European Journal of Information Systems* 15, (2006): 542-555.

Wakefield, R.L. and Whitten, D. "Examining User Perceptions of Third-Party Organization Credibility and Trust in a E-retailer" *Journal of Organization and End User Computing* 18, no. 2, (2006): 1-19.

Wambugu, S. "Beating Digital Crooks at Their Game" *Daily Nation*, July 11th, (2009), available at: http://www.nation.co.ke/business/news/-/1006/622676/-/view/printVersion/-/sxr58kz/-/index.html

Wang, Y.D. and Emurian, H.H. "An Overview of Online Trust: Concepts, Elements, and Implications" *Computers in Human Behaviour* 21, (2005): 105-125.

Wang, Y.-S., Lin, H.-H. and Luarn, P. "Predicting Consumer Intention to Use Mobile Commerce" *Information Systems Journal* 16, no. 2, (2006): 157-179.

Webster, J. and Martocchio, J.J. "Microcomputer Playfulness – Development of a Measure with Workplace Implications" *MIS Quarterly* 16, no. 2, (1992): 201-226.

Webster, J. and Trevino, L.K. "Rational and Social Theories as Complementary Explanations of Communication Media Choices" *Academy of Management Journal* 28, no. 6, (1995): 1544-1572.

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

Williams, L.J., Edwards, J.R. and Vandenberg, R.J. "Recent Advances in Causal Modeling Methods for Organizational and Management Research" *Journal of Management* 29, no. 6, (2003): 903-936.

Williamson, O.E. "Calculativeness, Trust, and Economic Organization" *Journal of Law and Economics* 30, (1993): 131-145.

Willis, G. *Cognitive Interviewing: A How-to Guide,* Research Triangle Institute, (1999), available at: **http://www.mrandosciasclass.net/resources/Cognitive+Interview+Manual.pdf**

Willox Jr., N.A. and Regan, T.M. "Identity Fraud: Providing a Solution", *Journal of Economic Crime Management*, 1, no.1, (2002):

Wolfinbarger, M. and Gilly, M.C. "Shopping Online for Freedom, Control, and Fun", *California Management Review* 43, no.2, (2001): 34-55.

Wu, J.-H. and Wang, S.-C. "What Drives Mobile Commerce? An Empirical Evaluation of the Revised Technology Acceptance Model" *Information and Management* 42, (2005): 719-729

Xie, E., Teo, H. and Wan, W. "Volunteering Personal Information on the Internet: Effects of Reputation, Privacy Notices, and Rewards on Online Consumer Behaviour" *Research* 18, no. 4, (2004): 336-355.

Xu, H. and Teo, H. "Alleviating Consumers' Privacy Concern in Location-Based Services: A psychological Control Perspective" in *Proceedings of the Twenty-Fifth International Conference on Information Systems* (2004): 793-806.

Yang, Z. and Jun, M. "Consumer Perception of e-Service Quality: From Internet Purchaser and Non-Purchaser Perspectives" *Journal of Business Strategies* 19, no.1, (2002): 19-41.

Yoon, C. and Kim, S. "Convenience and TAM in a Ubiquitous Computing Environment: The Case of Wireless LAN" *Electronic Commerce Research and Applications* 6, (2007): 102-112.

Yousafzai, S.Y., Pallister, J.G. and Koxall, G.R. "A Proposed Model of E-Trust for Electronic Banking" *Technovation* 23, (2003): 847-860.

Yu, J., Ha, I., Choi, M, and Rho, J. "Extending TAM for a T-Commerce" *Information and Management* 42, no. 7, (2005): 965-976.

Zedeck, S. "An Information Processing Model and Approach to the Study of Motivation" *Organization Behaviour and Human Performance* 18, (1977): 47-77.

Zinkewicz, P. "Identity Theft" *Rough Notes* 150, no. 6, (2007): 120-126.

Zhang, X., Prybutok, V. and Huang, A. "An Empirical Study of Factors Affecting E-Commerce Satisfaction" *Human Systems Management* 25, (2006): 279-291

Zmud, R. and Boynton, A. "Survey Measures and Instruments in MIS: Inventory and Appraisal" *The Information Systems Research Challenge: Survey Research Methods* 3, (1991) Harvard Business School, Boston, MA.

Zorkadis, V. and Donos, P. "On Biometrics-Based Authentication and Identification From a Privacy-Protection Perspective: Deriving Privacy Enhancing Requirements" *Information Management and Computer Security* 12, no. 1, (2004): 125-137.

Zucker, L.G. "Production of Trust: Institutional Sources of Economic Structure, 1840-1920" *Research in Organizational Behaviour* 8, (1986): 53-