uOttawa

L'Université canadienne
Canada's university

FACULTÉ DES ÉTUDES SUPÉRIEURES ET POSTOCTORALES

uOttawa

L'Université canadienne
Canada's university

FACULTY OF GRADUATE AND POSDOCTORAL STUDIES

Jennifer Duff

AUTEUR DE LA THÈSE / AUTHOR OF THESIS

M.A. (Criminology)

GRADE / DEGREE

Department of Criminology

FACULTÉ, ÉCOLE, DÉPARTEMENT / FACULTY, SCHOOL, DEPARTMENT

Normalizing Extraordinary Technologies in the Risk Society: Perceptions of Biometric Passports in Canada

TITRE DE LA THÈSE / TITLE OF THESIS

Micheal Kempa

DIRECTEUR (DIRECTRICE) DE LA THÈSE / THESIS SUPERVISOR

CO-DIRECTEUR (CO-DIRECTRICE) DE LA THÈSE / THESIS CO-SUPERVISOR

EXAMINATEURS (EXAMINATRICES) DE LA THÈSE / THESIS EXAMINERS

Christine Bruckert

Daniel dos Santos

Gary W. Slater

Le Doyen de la Faculté des études supérieures et postdoctorales / Dean of the Faculty of Graduate and Postdoctoral Studies

Normalizing Extraordinary Technologies in the Risk Society: Perceptions of Biometric Passports in Canada

Jennifer Duff

Thesis submitted to the
Faculty of Graduate and Postdoctoral Studies
In partial fulfillment of the requirements
For the MA degree in Criminology

Department of Criminology
Faculty of Social Sciences
University of Ottawa

Your file Votre référence
ISBN: 978-0-494-61282-8
Our file Notre référence
ISBN: 978-0-494-61282-8

Acknowledgements

First and foremost I would like to thank my parents, Mike and Cathy, my brothers, Stephen and Derek, and my close friends for their unwavering support in all of my undertakings.

Secondly, I would like to thank Jane Barker, Norma Jo Baker, and Greg Brown from Nipissing University for providing me with the information, encouragement, and support that I needed to pursue graduate studies.

I would also like to express my appreciation for my thesis supervisor, Michael Kempa, who always provided me with positive feedback and helpful suggestions that enabled me to complete my thesis in a timely fashion.

Special thanks to my thesis committee members: Cheryl Webster, Daniel Dos Santos, Christine Bruckert and Dominique Robert.

To my fellow graduates and classmates: I have thoroughly enjoyed sharing the experiences of graduate school with you and wish you all the best in your future endeavors.

Table of Contents

List of Tables

Abstract

Contemporary society is plagued with perceived risks and feelings of uncertainty. In traditional societies, people relied on kinship, norms, and shared identity to establish ties and manage the risks of the collective. Technology is increasingly sought to manage risks as present day society is thought to be facing manufactured, virtual, and borderless risks not experienced in previous eras. Technologies, such as biometric identification systems, operate within a network society capable of processing and disseminating information like never before. The science behind the various types of technological systems enable greater risk detection but also reinforce the public's fear of crime as these technologies highlight the omnipresence of risk. Greater awareness of risk ultimately heightens fear of crime and creates anxiety amongst the public towards expert systems that cannot effectively manage the risks they detect. Van Loon (2000) identifies the increasing reliance on technology to manage risks at a time when science is facing severe criticism as a central paradox within the risk society. Therefore, the focus of the current study is to expand the current knowledge regarding how extraordinary technologies that were once used to identify immigrant and marginalized populations have permeated all facets of society. More specifically, the current study examines biometric technologies that are increasingly used to securitize the identity of the whole population, to control access to restricted areas, and to secure items of personal property. To investigate the normalization of extraordinary technologies and the nature of the hypothesized ambivalent relationship people have towards science, the current study utilizes a group-administered student questionnaire. Students' were asked about their perceptions of risk, safety, and biometric technologies in order to gain a greater understanding of the factors that contribute to the acceptance or non-acceptance of biometric passports in Canada before their issuance in 2011. In the current study it was hypothesized that people who possessed certain individual characteristics such as anxiety towards expert systems, previous victimization, negative perceptions of safety, or a lack of familiarity with biometrics would be less accepting of biometric passports. It was also hypothesized that finger scans would be the biometric identifier of choice as finger scans have been slowly integrated into multiple facets of society over a long period of time. Trust in expert systems was found to be of central importance in the acceptance of finger scan passports, while potential discriminatory consequences of biometric passports contributed to the ambivalent relationship people have towards science. Despite their association with criminal investigations finger scans were preferred over the use of facial scanning for various purposes including for use on biometric passports.

1 INTRODUCTION

The world has been brought together by communication, information and transportation technology. Advances in transportation technology have brought countries and continents together like never before enabling travel both nationally and internationally. Travel has become a popular leisure activity and a part of everyday business transactions. People who are deemed to be low-risk travelers enjoy a freedom of mobility once unimagined. Along with the steady increase in travel comes the perceived need for heightened security measures to ensure the safety of travelers and countries that welcome travelers through their borders. Within this technological revolution individuals are increasingly required to prove their identity to gain access to privileges and entry into certain areas. Technological solutions are often sought to manage territories and populations as governments are becoming increasingly concerned with regulating flows of travelers crossing borders (Ceyhan, 2006; Salter, 2006).

1.1 **Thematic Issue: Normalizing Technology & Criticizing Experts**

The process of discerning between who can and cannot pass through a country's border is shifting from a human based identification process to an increasingly automated system of classification (Lyon, 2005). Prior to the advancement and implementation of various identification technologies, a border agent would verify a traveler's identity by visually comparing a person's face to a picture on an identification document. The identification process was based on the agent's training, experience, discretion and standard procedures. Identification technologies, however, assess a traveler's dangerousness by comparing the traveler's information with information from crime, terrorist, and border files in order to categorize a traveler as 'safe' or 'risky' (Ceyhan, 2006). This automated system of identification and classification highlights a technological shift that needs to be examined in terms of user acceptance of expert

technologies and what this says about the risk society. Citizens are urged to trust expert systems based on the performance of the technology and the legitimacy and professional standards required to be an expert. However, Merryn Ekberg (2007) asserts that the trust/skepticism dichotomy is one of the central contradictions of the risk society. Therefore, the current study seeks to expand the current knowledge about the issue of trust in expert systems of technology. More specifically, the study will examine the proliferation of risk definitions, the increasing awareness of uncertain risks and individual's trust in expert systems of technology such as biometric passports.

According to Giddens (1996) and Ekberg (2007), among others, the lack of consensus among experts regarding how to effectively manage the increasing risks of contemporary society may have damaged the authority of experts and expert systems. The timing of this skepticism is particularly interesting as it is occurring during a time when extraordinary technologies that were once used to identify asylum seekers and marginalized populations are expanding their scope to include entire populations. Expert technologies are also used throughout society to control access to restricted areas or to securitize items of personal property. Therefore, the current study will examine the normalization of extraordinary technologies (such as biometric passports) for managing risks during a time when science and experts are being criticized by citizens and other experts for not effectively managing these risks.

1.2 **Empirical Issue: Biometric Passports**

Simply stated a biometric is a measurement of a physiological feature or behavioural characteristic used to verify one's identity (Ng-Kruelle, Swatman, Hampe, & Rebne, 2006). Unique biometric identifiers include: finger prints, iris scans, facial scans, hand geometry, voice recognition and gait. Globally interoperable biometric passports as promulgated by the

International Aviation Organization (ICAO) contain a contactless chip that stores the bearer's name, date of birth, place of birth, gender, passport number, date of issuance and expiration along with a digital photograph (Bureau of Consular Affairs, 2007).

People who support and encourage the implementation of biometric passports in Canada tout the passport's ability to efficiently manage people traveling through borders. On February 27, 2008 Canadian Finance Minister Jim Flaherty announced a $165-million spending package aimed at enhancing border security, which included the issuance of higher-security electronic passports starting in 2011 (Blanchfield, 2008). Complete details regarding Canadian biometric passports have yet to be specified. This means that there is still time to conduct valuable research into public perceptions regarding the use of expert technologies for identification purposes. Technological advances have quickly transformed the way we travel and the way we identify and detect risks at the border. This proliferation of expert systems for managing risks comes at a time when scientific expertise faces criticism for not effectively managing risks (Giddens, 1996). The conflicting opinions among experts cause an endemic of insecurity: with increasingly fewer traditions and established group norms for guidance, individuals are left to face risks alone or turn to experts and professional advisors (Garland, 2003). Experts are increasingly sought to manage these risks despite some of the negative ramifications associated with expert systems of technology. This ambivalent relationship that people have towards science and technology will be explored throughout the current study.

Technologies, such as biometric identification systems used in conjunction with electronic passports, are often seen as innovative and efficient ways to identify and verify one's identity. However, this type of identification system has various societal, ethical, legal, and political implications. Biometric identification systems have discriminatory ramifications for certain

members of society including people who do not want to submit biometric data because of religious beliefs or who have physical disabilities that prevent them from submitting biometric data for identification purposes. Meanwhile, privacy conscious individuals are concerned about issues of physical and informational privacy as well as the potential for the information to be improperly used to track individuals. While privacy is a major issue of concern regarding the implementation of biometric passports in Canada, various other negative implications act as sources of concern as well. One issue is the temporal nature of biometric data. Physical characteristics develop and may even change over time (Current Security, 2003). The sophistication of biometric passport readers raises questions regarding how often individuals would have to re-submit biometric information for the issuance of a new passport in order to keep the biometric data accurate. There are additional concerns regarding practicality like for example how an individual would obtain a passport if that individual's particular physical characteristic used for biometric identification became severely damaged and immeasurable. This leads to another concern of biometric passports, irrevocability (Current Security, 2003). If biometric data is stolen or compromised, the affected individual cannot change the physical characteristic from which the data was collected. Therefore, an important implication to consider is the fact that once biometric data is compromised it is impossible to return to a totally secure situation (Current Security, 2003).

Within the risk society there is a contradiction in terms of the increasing use of expert technologies for managing risks during a time when experts face severe criticism for not effectively managing these risks. Experts are tasked with having to maintain public confidence by effectively managing risks while safeguarding users' biometric information and creating alternatives for those unable to submit biometric data.

1.3 Case Study: Students in first year courses at the University of Ottawa

Authors such as Anthony Giddens and Merryn Ekberg suggest that confidence in scientific authority is decreasing due to a lack of consensus among experts. However, biometric technologies are increasingly being sought for their ability to efficiently identify and verify a traveler's identity. Therefore, a group-administered questionnaire was distributed to students in first year courses at the university of Ottawa to explore this ambivalent relationship and to empirically expand the current knowledge regarding perceived risk, heightened security, and the normalization of extraordinary technologies.

Countries such as Germany, Russia and the United States have implemented a top down approach of governance through identification documents without any feedback from the public, the mandated users of the proposed biometric passports. Examining public perceptions regarding the use of biometric passports will allow for the identification of the issues that the public agrees/disagrees with enabling insights into the way people perceive risk and the need for security. This will allow for a greater understanding of the specific circumstances where people are willing to use various types of biometric identification methods. Therefore, the current study surveys a sector of the proposed users of biometric passports, a largely ignored but rather important sector affected by the implementation of biometric passports. A group-administered questionnaire is utilized in this study to measure perceptions of students in first year courses at the University of Ottawa toward expert technologies such as biometric passports in order to determine how biometric passports would be received in Canada in terms of the issues highlighted above.

Stemming from the thematic questions of the current study, respondents were also asked a series of sub-questions relating to their preferred biometric identifier as well as their opinions

regarding how the implementation of biometric passports would influence policy in Canada. These sub-questions were included in the questionnaire to solicit responses on a wide range of biometric issues to gain a better understanding of people's perceptions of biometric passports and to supplement the responses to thematic questions.

What follows is a brief overview of the information and topics discussed in the various chapters of this paper. Following the introduction, the first major chapter of the current paper serves as a contextual overview of the theoretical framework used to guide the current study. This first chapter briefly describes the transition from the reliance on welfare state services to neo-liberal practices of individualism and market competition as well as the shift in trust relations from trust in the established norms of traditional society to trust in abstract systems under neo-liberalism. This chapter also discusses Garland's assertion that science is increasingly being delegitimatized as well as the hypothesized ambivalent relationship people have towards science that is highlighted by Van Loon (2000). The discriminatory nature of airport security reliant on risk- based calculations, highlighted by O'Malley (2006) is also explored. In terms of theoretical relevance, Merryn Ekberg's conceptual model of the six parameters of the risk society sheds light upon the nature of risk and feelings of safety and security in contemporary society. New understandings of risk along with the proliferation of risk definitions highlights the shift from trust in traditional facework commitments such as religion and shared identity to trust in abstract systems and faceless commitments such as money and technology (Ekberg, 2007). Within the risk society, this type of trust relationship highlights an interesting contention within the politics of the risk, whereby the use of technology approved by unelected scientists threatens the notion of democracy (Garland, 2003). The current research study seeks to explore the nature of the relationship people have towards technology by identifying the purposes for which people

are willing to provide biometric identification as well as some of the reasons associated with the acceptance of biometric passports. The current study also explores whether anxiety towards expert systems or experiences of previous discrimination contribute to people's concern about the potential discriminatory consequences of biometric passports. Many issues and concerns about biometric passports have already been realized in other countries yet the continued implementation of biometric passports has not faced considerable resistance from the mandated users of the passports. This particular theme relating to Van Loon's hypothesized ambivalent relationship that people have towards science and technology is highlighted within the risk society and is examined throughout the current study.

After examining the risk literature and gaining a better understanding of the problems and issues surrounding risk, the network society literature is examined in order to gain a greater understanding of how the technological solutions sought to manage these risks operate, as well as their effectiveness and unintended consequences. Within the network society, communication and information technology operate by translating all inputs into a common digital language to be stored, processed, and disseminated throughout various nodes of the network. Felix Stalder (2006) contends that networks are quickly becoming the predominant form of organizing various aspects of social life because the flexibility and efficiency of networks allow for a level of processing and disseminating of information never before seen. Biometric passports operate in a network that collects, stores, processes and distributes information with the objective of increased security by ensuring a very high standard of proof of identity (Ceyhan, 2006). Within the network society the power of technology has enabled greater risk detection and interception. These technologies however, also create more risks, unforeseen and otherwise, that create skepticism towards expert systems of identification.

A major theme of the current study relates to how extraordinary technologies, that were once merely themes in futuristic movies, became integrated into everyday lives of individuals. More specifically, how the use of biometric technologies has come to permeate multiple facets of society to secure borders, workplaces, and items of personal property. Ceyhan (2006) contends that the integration of these technologies is premised upon effective security management and the ability of these technologies to permeate various domains of society to familiarize users with the technology. People accept biometrics for various reasons including: convenience, ease of use, efficiency, accuracy and increased security (Reid, 2004). Therefore, along with examining the reasons associated with acceptance or non-acceptance of biometric passports, the current study identifies whether respondents prefer finger or facial scans for use on biometric passports. This particular question probes the depth of integration that finger and facial scans have achieved and how accepting people are of their usage.

Expert systems of identification are increasingly sought to manage risks during a time when science and technology face severe criticism. To add contextual relevance, an examination of the both biometric technologies considered for use on passports (finger and facial scans) as well as a discussion of passports in general is included in the first major chapter of this paper. The biometric technologies are examined in terms of their perceived advantages and disadvantages for police and citizens, as well as their previous and current usage. The importance of passports is discussed in terms of state-building and citizenship, followed by a discussion regarding the possible implications stemming from identification documents such as social sorting and state surveillance. This particular chapter serves to situate the current study within the context of the risk discourse and the network society theory. Within this context, the current study examines the case of the biometric passport to determine whether questionnaire

respondents have an ambivalent relationship towards science in this instance. This study will also identify respondents' preferred biometric identifier and expand the current knowledge regarding the technology's level of integration throughout society.

The methodology chapter outlines the various methodological decisions made by the researcher that guided the current study. This quantitative study utilized a group-administered paper questionnaire distributed to students in first year courses at the University of Ottawa in order to gain a greater understanding of how future users of the proposed Canadian biometric passport perceive the technology, its implications, and its effectiveness. The computer program SPSS (Statistical Package for the Social Sciences) was used to create and maintain an electronic database containing students' responses to the questionnaire and was also used to create various indexes and to analyze the findings by running various statistical tests of significance and association. The methodological decisions made in the current study contribute to a unique approach of examining users' perceptions about biometric passports prior to implementation.

The results chapter displays a range of tables of results and outlines the various findings of the current study. The current study was able to conclude that finger and facial scans received the highest support for use as methods of identification at border crossings, that students preferred finger scanning technology over facial scanning, and that feelings of national vulnerability were associated with a greater acceptance of biometric passports. Distrust in expert systems was highlighted as a major reason for not accepting biometric technologies while the potentially discriminatory implications of biometric passports was found to be further evidence of the ambivalent relationship people have towards science and technology.

The subsequent chapter provides a detailed discussion of the findings reported in the preceding results chapter. The creation and maintenance of trust between citizens and the

technologies that are created to manage them is a major component for the acceptance of finger scan passports. Familiarity and experience with biometric technologies helps establish trust towards these types of systems however, personal vulnerabilities such as being concerned that biometric data could be used to track people creates anxiety towards expert systems of technology. These and other themes relating to the normalization of extraordinary technologies and the ambivalent relationship people have towards science and technology are highlighted and discussed in detail.

The final chapter serves as a summary of the thematic findings and issues regarding the normalization of extraordinary technologies and the nature of the relationship people have towards science and experts. This chapter concludes with practical recommendations including: 1) continued in-depth research into the area of trust in expert systems and other reasons associated with the acceptance of biometrics; 2) the continued challenging of technology in order to fuel advancements that will increase efficiency and mitigate discriminatory consequences; and 3) the democratization of scientific decisions. The trade-off between national security and individual rights has various implications for the notion of democracy. However, the public could greatly benefit from a democratization of expertise, which would ultimately bring the biometric debate out into the public.

2 LITERATURE REVIEW

2.1 **Theoretical Framework**

Before examining the risk society specifically, an overview of the historical conditions and practices that gave rise to our present day experiences will be discussed in order to give historical relevance to the emergence of the risk society.

The period between the 1950s and the 1990s was characterized by a steady increase in crime as well as rapid social and economic changes (Garland, 2001). In the welfare state, it was the state's responsibility to protect the economic and social wellbeing of its' citizens (Welfare State, 2009). The welfare state ushered in concern for social equality, social security and social justice based on the principles of equitable distribution of wealth and equal opportunity. State services were designed to meet the needs of adequate housing, healthcare, basic education, social work as well as income support (Welfare State, 2009). During this time communal structures such as the church, family and community gave order to people's lives. The church was instrumental in providing meaning and purpose in life while the community and extended family relations gave people a sense of identity (Beck, 1992). According to Giddens (1990), trust in these types of traditional societies with high levels of direct interaction is embedded in kinship, religion, and established customs. This type of trust relationship, based on facework commitments, offers individuals a sense of security and group belonging (Ekberg, 2007). However, the structure of the family and the notion of community became severely dislocated as people became dependent upon the social services of the welfare state instead of seeking out assistance from family members, moneylenders or low-paying jobs (Garland, 2001). Furthermore, the institutions of the welfare state uncovered more unmet needs than the

institutions could adequately address which undermined the legitimacy of the welfarist forms of government (Garland, 2001).

It was also during this time that the public accepted crime as a normal social fact that could potentially affect anyone (Garland, 2001). Previously crime was considered a problem that affected the poor but was increasingly becoming a potential problem for anyone, regardless of class. As crime rates continued to grow the public began to lose confidence in experts' ability to prevent crime and create effective policies (Garland, 2001). Over the decades, the public's views towards crime and crime control shifted dramatically. The public increasingly came to accept the increasingly high crime rates but felt the need to establish control over risks and became increasingly impatient with the criminal justice system's failure to control dangerous individuals (Garland, 2001).

By the 1970s, concerns regarding the economic sustainability of the welfare state were also growing. Government borrowing was overstretched to maintain public expenditure and increasingly high levels of personal taxation were required to sustain this (Pratt, 1999). Individual freedom and autonomy threatened the structure of traditional society (Beck, 1992) as people became aware that their tax dollars were paying for state services that they may never use (Garland, 2001). The welfare state began to break down as social issues including increased crime, worsening race relations, and the breakdown of family and traditional values were changing people's actuarial interests (Garland, 2001).

Market forces, that changed the dynamic of supply and demand, undermined the institutions of the welfare state. Within neo-liberalism, these market alternatives enabled people to pay for better education, healthcare, private security, and housing (Garland, 2001). Within neo-liberalism the state plays a minimalist role as markets are deemed to be better ways of

organizing economic activity based on competition, efficiency and choice (Larner, 2000). In place of the collective responsibility of the social, there is increasing importance placed on individual responsibility. Similarly, instead of investing in social provision and the inclusion of the economically disadvantaged, greater emphasis was placed on the need to effectively manage problem populations (Garland, 2001). Advancements in communication and transportation technologies have expanded the parameters of risk and thus of risky people. Within the market of expertise, competition to provide risk management services is maximized as both public and private sector security compete to offer expert advice and services (O'Malley, 2004).

Under neo-liberalism the responsibility for general risk management has shifted as did the nature of trust relations. Trust in post-traditional societies is increasingly embedded in faceless commitments such as symbolic tokens (money) and expert systems (technology) (Ekberg, 2007). Trust in these faceless commitments is rooted in professional codes of practice, reputation and the performance of unfamiliar abstract systems used to manage risk (Ekberg, 2007). As the dynamics of trust shifted people increasingly began to lose confidence in many of the welfare state's institutions.

At times the welfare state appeared to be the problem rather than the solution; however according to Garland (2001), the welfare state established core institutions that ultimately shaped late modernity and ushered in a new culture of individualism and social democracy. The infrastructure that welfarism was built upon was not completely abolished but simply directed by a new style of management that provided incentives to discourage dependency (O'Malley, 2004). The notion of assistance was not completely abandoned under neo-liberal politics however, people were no longer 'entitled' to support. Assistance for unemployed people, for example, is provided on the basis of mutual obligation. Unemployed people are able to receive 'allowances'

while improving their job skills by attending skills training or resume workshops (O'Malley, 2004). Provisions within neo-liberalism are designed to encourage people to become more independent and responsible for their own future (O'Malley, 2004).

The welfare state also opened up various avenues for the operation of expert judgment. The knowledge, training and specialized skills employed by previous 'social' experts led the way for the neo-liberal experts who employ these skills to manage risk (Rose, 1996). The social workers and psychiatrists who previously attempted to cure their clients are now encouraged to use their skills and judgment to minimize the risks of their clients (Rose, 1996). Within the criminal justice system risk is often the principle upon which funds and other resources are allocated. Criminal justice professionals also employ risk assessment in order to assign inmates to effective programming and to determine if and when inmates are safe to release (O'Malley, 2004).

Risk and risk management have changed the way society is organized and the way people live their lives. For Ulrich Beck, risk is the defining feature of modern society. "Pre-modern dangers were attributed to nature, gods, and demons. Risk is a modern concept. It presumes decision-making" (Beck, 2002, p.40). What distinguishes modern risks from the dangers that plagued pre-modern societies, according to Beck (1992), is that the risks of contemporary society are largely man made and increasingly global. Pre-modern dangers included floods and famines whereas the man made risks in current society, such as threats of terrorism and global warming, are the result of human action (Beck, 2002). These new man made risks expanded the parameters of risk, which ultimately led to the creation of new technologies to manage them. As individuals become increasingly free to govern themselves through choice, they are becoming increasingly aware of their ability to demand better risk management tools (O'Malley, 2004). Both public and

private forces compete in a market of expertise to meet the needs brought about by increasingly global risks. The current study examines students' perception of these risks as well as their attitudes towards the need for heightened measures of security such as biometric passports. As identified above, trust in facework commitments and state institutions has shifted whereby individuals are increasingly urged to trust in symbolic tokens and abstract systems. The current study explores students' trust in expert systems and their associated perceptions regarding the use of biometric passports. The current study also examines the notion of risk in terms of people's perceptions of risk and their resulting attitudes towards the need for heightened security. Additionally, the concept of risk in terms of the 'risk society' is explored and discussed in detail below.

2.1.1 The Risk Society

Contemporary society has been characterized as a society of risk by various authors and theorists alike. Sociologists Ulrich Beck and Anthony Giddens claim that we are living in a risk society or a reflexive age of modernity characterized by low-probability, high consequence technological risks. Reflexivity refers to "a process of continuous monitoring and surveillance, and of making adjustments as new information and revised knowledge become available" (Ekberg, 2007, p.354). Within the reflexive age of modernity there are a whole host of occupational specialists who measure and manage risk. According to David Garland (2003), risk is a calculation, a problem, a source of insecurity, is objective and subjective, is scientifically knowable and socially constructed. Objective risk is calculated using scientific data to determine the actual risk of a particular occurrence whereas subjective or socially constructed risk is based on perceived impressions (Garland, 2003). Ulrich Beck asserts that: "if people experience risks

as real they are real as a consequence" (Beck, 1992, p.77, emphasis in original). Alternatively, Baruch Fischhoff argues that:

> what is commonly called the conflict between actual and perceived risk is better thought of as the conflict between two sets of risk perceptions: those of ranking scientists performing within their field of expertise and those of everybody else. (Royal Society 1992, p.97).

At times, subjective perceptions of risk dominate while scientific data faces severe criticism, a theme that will be addressed throughout this paper. It is not uncommon for people to place greater trust in their own personal experiences or that of their friends and family than in claims made by experts (Garland, 2003). Research suggests that people tend to overestimate the frequency of low-probability, high consequence events such as plane crashes and underestimate the risk of high probability, low consequence events such as accidents in the home or on the road (Garland, 2003). Risks do not exist outside of our knowledge of them as "they are the product of future-oriented human calculations-assessments made by people in the face of an uncertain world and the possibilities that it holds for them" (Garland, 2003, p.52). Risk therefore exists within the realm of uncertainty at the point where certain knowledge ends.

Merryn Ekberg (2007) highlights six parameters of the risk society in an attempt to develop a unique perspective regarding the nature of risk in contemporary society. The first of six parameters is the omnipresence of risk characterized by an increasing awareness of risk and uncertainty. As people become more aware of risks they increasingly seek out new ways to manage them. Van Loon (2000) and other risk society theorists seek to understand the contradiction between the increasing use of science and technology to measure risks while the method of science is increasingly being delegitimatized because of its failure to effectively manage these risks (Beck, 1992; Ekberg, 2007; & Garland, 2003). Increasing threats to identity

and the risks associated with the collapse of traditional norms cause dislocation and disintegration within society. Lash (1994) argues that risk created a common feeling of vulnerability whereby the collective feelings of insecurity gave rise to a new ethos of a risk culture. While not yet empirically validated, it has been hypothesized that people have an ambivalent relationship with science in the risk society as not only is science itself facing criticism (Giddens, 1996) but expert authority is also being questioned (Eckberg, 2007). At times people see scientific methods as the best way to manage risks while at other times people fear the uncertain risks identified by new technologies and the social, legal, and cultural impacts of these technologies. A discussion of the potential consequences of employing technological solutions to manage social problems follows.

The emergence of a new understanding of risk, the second parameter of the risk society, highlights the shift in focus from natural risks such as floods and earthquakes to manufactured technological risks associated with advances in nuclear and biomedical technologies (Ekberg, 2007). Technological advancements brought unintended consequences that threatened modernity after the collapse of the welfare state and its institutions. These manufactured risks were the result of technical power used to manipulate nature (Ekberg, 2007). This aspect of the risk society highlights the inherent problem with technological solutions to natural or social problems: it is possible that the same technology used to manage a particular risk could be manipulated and used in a manner other than the way it was intended thus creating more risk. For example, if a database that contains passport holder's biometric data was breached, this would create risky situations for the people who had their identity stolen and to those countries where the thieves intend to enter using the stolen biometric data. Therefore, it is possible that technology can cause various unforeseen consequences that the technology itself cannot remedy.

"The risks of the risk society are not only problems *of* technology, they are also problems *for* technology" (Ekberg, 2007, p.352, emphasis in original). The problems created by expert systems for managing risk are more easily discernable than are the potential problems the technologies seek to manage. The problems created by technologies designed to manage risks therefore reinforce the ambivalent relationship people have with science and expert technologies.

The proliferation of risk definitions is the third parameter of the risk society as outlined by M. Ekberg (2007). Contemporary risks can be local or global, individual or collective, real or constructed, natural or manufactured and as such, are difficult to empirically define (Ekberg, 2007). Risks are calculated based on the outcomes of choices made by human beings, which results in a wide range of risk definitions. Risk experts agree that risks are related to threats, hazards, and dangers but do not agree on how risk is actually defined (Ekberg, 2007). Sociologist Ulrich Beck (1995) argues that a risk is something for which private insurance can be purchased in order to manage its consequences whereas private insurance cannot be obtained to manage a threat. Writing from a realist perspective, Geoff Wells (1996) describes risk as the possibility of an unpleasant incident and defines hazard as the situation that may initiate such an incident. Anthropologist Mary Douglas (1992) however, makes a distinction between hazards and risks as she describes hazards as pre-existing situations and risks as culturally contingent upon value-judgments of human perceptions. These competing risk definitions create barriers to effective risk communication as well as efficient risk management. With the increasing use of private sector institutions in risk management it would be beneficial to have consensus regarding the definition of risk to ensure effective risk management. However, communication, information and transportation technology are continuously advancing and creating new risks thus expanding the parameters of risk. The notion of risk has numerous historical and cultural

interpretations, which makes it difficult for experts to agree upon how to effectively manage the risks of contemporary society.

The fourth parameter of the risk society, the reflexive orientation to risk, refers to a level of flexibility possessed by individuals and institutions that allow them to respond to risk and uncertainty as new knowledge is acquired (Ekberg, 2007). No longer constrained by religion or tradition, individuals seek information in order to examine available courses of action. Reflexivity enables individuals and institutions to manage their risk environments in times of changing and uncertain knowledge.

The relationship between risk and trust highlights the fifth parameter of the risk society. According to Giddens, it is the emergence of new expressions of trust that characterizes the reflexive age of modernity (Ekberg, 2007). In traditional society trust is rooted in kinship, shared identity, religion, and customs. Traditional society is characterized by trust in facework commitment where levels of direct interaction and communication are high, which gives individuals a sense of group belonging (Giddens, 1990). Alternatively, trust in abstract systems or faceless commitments is the trust relationship that characterizes the reflexive age of modernity. Trust in abstract systems includes trust in symbolic tokens (like money) and trust in expert systems (technology) (Giddens, 1990). Faceless trust is characterized by trust in an unfamiliar, sometimes anonymous, distant social system whereby individuals trust the legitimacy and credentials of professionals based on qualifications, accreditation, reputation and performance (Giddens, 1990). However, Ekberg (2007) asserts that the relationship between trust and skepticism is one of the main contradictions of the risk society. According to Ekberg (2007), a lack of consensus among experts and truth claims has damaged the image of science as an all-knowing and infallible discipline. According to Van Loon (2000) and Giddens (1996), science

lost some of its dominant authority, as the opinions of experts were no longer considered the only legitimate truth (Ekberg, 2007). This elicits an important research question regarding the hypothesized ambivalent relationship that people have towards science and expert authority. *Research Question 1*: In what types of situations are people willing to provide biometric data for identification purposes during a time when science and expert authority is being questioned in the risk society?

In the current technologically networked society there are increasing concerns regarding security threats, fraud and identity theft and as such people are generally willing to accept the use of biometric technologies to gain access to personal property and services (Jain, 2007). Marketers tout the long established history of use of fingerprints for identification purposes and therefore believe that users who wish to gain access to certain privileges will accept the use of fingerprint technology (Nanavati, Thieme & Nanavati, 2002, p.58). Proponents of facial scanning technologies advocate support for computerized facial recognition systems based on the fact that on a daily basis people use facial recognition to verify another's identity based on the characteristics of his/her face (Hribernig, & Weinzierl, 2006, p.86 & Reid, 2004, p.105). However, biometric technologies did not have sufficient time to mature before being thrown into the national spotlight after 9/11 (National Science &Technology Council, 2008). Instant experts emerged with a limited understanding of how to introduce biometric technologies to the public or how to ensure privacy. What resulted was an anxious public unsure of how biometric technologies operated or how their biometric information would be protected. The lack of familiarity with and understanding of biometrics created distrust towards the technology and the experts, some of which still exists today (NSTC, 2008).

The discussion above regarding trust in expert technologies brought forth the following research question in the current study:

Research Question 2: Do individual characteristics such as frequency of travel, familiarity with biometrics, anxiety towards expert systems, perceptions of safety or previous victimization contribute to the acceptance or non-acceptance of biometric passports in the risk society?

Related to the acceptance of biometric technologies are notions of perceived level of safety and anxiety towards expert systems of identification. Feelings of vulnerability are often associated with victimization, a heightened fear of crime and disorder, but also encompasses discrimination, as well as perceptions of safety associated with walking/being alone in various areas both before and after dark (Nugent &Van Daele, 2006). Individuals who feel vulnerable in terms of discrimination and level of perceived safety will likely be more willing to accept the use of heightened security measures as an attempt to enhance safety at the nation's border which will subsequently serve to protect the citizens of Canada. Those individuals who have had to experience the consequences of victimization are more likely to fear crime and future victimization and would therefore be more open to trusting new technologies that may be able to provide enhanced security in general (even if the security measure will not protect them from the specific crime of which they were a victim of) (Leiker, 2006). Additionally, the fear of crime feedback loop heightens fear of crime and its related research, whereby research into a particular area maintains the fear associated with that area and is used to justify governance (Lee, 2001). Fear of crime is therefore a construction that is reinforced by the feedback loop since people have to be aware of crime to fear it. Threats to national security have been increasingly discussed since September 11, 2001 and those individuals who are more fearful of crime are more likely to view biometric passports as viable measures of security that will protect Canada's citizens.

Expertise is narrowly restricted to a small group of specialists working with classified information with little or no input from the democratic public (Liberatore, 2007). Implementing new technologies without educating the public creates suspicion and doubt amongst users as they wonder why biometric data is collected and begin to fear misuse of the data collected (Liberatore, 2007). A study conducted in the UK in 2006 reported that 35% of the participants had no prior awareness or knowledge of biometric technology (Furnell & Evangelatos, 2007). Of the 65% who stated prior awareness of biometric technology only 27% received this prior knowledge from an educational course compared to 48% whose awareness originated from a sci-fi movie (Furnell & Evangelatos, 2007). Individuals who are unaware of what biometric technology is or how it works may be reluctant to embrace its usage until a certain level of trust can be established between citizens and the creators of expert systems of technology.

The final parameter of the risk society outlined by M. Ekberg (2007) is the politics of risk. The ideological conflicts that characterize the reflexive age of modernity in which we currently live are concerned with increasing the quality of life, decreasing risks, and measuring and managing impacts of new technologies while maintaining safety and security (Ekberg, 2007). These conflicts and the methods proposed to manage them highlight the implications of using technology approved by scientists, such as social control and privacy infringements, which put our fundamental ideals of justice, equality and rights at risk (Ekberg, 2007). According to Beck (1992), power imbalances, the erosion of citizen's rights and decisions made by unelected scientists threaten the notion of democracy. Individuals and future generations are affected by the decisions made by scientists who do not consult the public. Beck (1992) suggests a cooperative framework where experts, counter-experts and non-experts could debate and participate in the decision-making process. There are many possible unintended consequences stemming from the

implementation and use of biometric technologies. However, there are also many social and ethical implications that could potentially be managed throughout the duration of use of biometric passports. Some of these potential implications and how they relate to the risk society are discussed below.

The creation of 'digital dossiers' or 'data doubles' has potentially serious implications regarding the protection of privacy (Solove, 2006). Politicians and journalists often reference George Orwell's *1984* when illustrating privacy concerns associated with the creation of informational databases. By amassing large amounts of information about people, information databases serve the purpose of social control while suppressing individuality and curtailing individual freedom (Solove, 2006). The collection of data in contemporary society however, is not conducted by a centralized authoritarian power seeking absolute control and domination in the Orwellian sense. Solove (2006) argues that information databases are capable of disempowering people by taking away their control of personal information and therefore advocates regulation regarding how data can be collected and used. The law must redefine the nature of the relationship between the information gatherer and the subject. The law must also stipulate the purposes for which information is gathered and limit information sharing between agencies (Solove, 2006).

Privacy advocates are apprehensive about the use of biometric passports because of issues of physical and informational privacy and the potential for the information to be used to track individuals within the risk society. Woodward (1998) contends that while no widely accepted definition of privacy and what it entails is available, when considering the use of biometrics, privacy includes aspects of autonomy including the "control we have over information about ourselves, control over who can sense us, [and] control over the intimacies of

personal identity..." (Woodward, 1998, p.390). As such, mandated users of the system should have the right to know how their biometric information is stored, who has access to it and what it is being used for. While many people are concerned with the privacy of their biometric data, others are concerned with the nature of the technology used for risk calculation as it has discriminatory lineage. Therefore a discussion of the discriminatory nature of technological risk calculation within the risk society follows.

Airport security has shifted from a rule-based approach to an approach to security that is based on risk calculation (O'Malley, 2006). Within a rule-based approach all travelers attempting to cross the border are considered to be equal risks and are therefore subjected to the same degree of scrutiny (O'Malley, 2006). Provided that no specific issue draws attention to a particular traveler, all travelers are considered moderate risks. The shift to a risk-based approach however, focuses more on the selective attention to high-risk travelers (O'Malley, 2006). Statistics are used to compile risk profiles and risk factors to aid in the identification of high-risk travelers. The issuance of biometric passports is also based on risk assessments that make it more difficult for certain individuals who fit particular profiles to obtain documentation.

The use of biometric identification technologies may be fairly recent but some would argue that the mentalities backing their usage are not. Weber and Bowling (2008) assert that border technologies are used to select, eject, and immobilize those without the required mobility rights based on risk parameters such as social capital and nationality thus fuelling global inequalities based on race and gender. The various parameters for exclusion and control have changed significantly since September 11, consequently increasing the demands on border security devices. At one time the definition of 'foreign' referred to a person who was not local; now it has become increasingly tied to national identity (Weber & Bowling, 2008).

> It is clear that at times of tumultuous social change, powerful economic and political forces have sought to regulate human mobility through governmental strategies in the local, national and transnational spheres. Mechanisms of control have evolved with changing technologies; where vagabonds were once whipped, branded and carted back to their home parish, they are now intercepted, documented biometrically, detained, deported and monitored electronically. (Weber & Bowling, 2008 p.371).

Accordingly, some authors argue that biometric identification systems are based on authentication methods that conceal the discriminatory process of identifying and distinguishing between risky and non-risky individuals (Ceyhan, 2006). O'Malley (2006) highlights the discriminatory nature of risk assessment as it is based on the cyclical process of racial profiling. Predictive risk instruments will ultimately reproduce the data from which they were premised upon, thus fueling the cyclical nature of risk assessment (O'Malley, 2006). For example, racial profiling is based on official conviction rates. Conviction rates are dependant upon the police working culture where risk assessments are based on assumptions of police officers who select who to target, by prosecutors who select which cases to proceed with and by judges who preside over the cases (O'Malley, 2006). What results is an increase in convictions for those targeted which re-affirms the basis for which they were targeted. Furthermore, this process of risk assessment offers no protection against the categories of people who could be dangerous but were not targeted or selected for prosecution. O'Malley (2006) asserts that not only does this result in a poor predictive risk assessment but its discriminatory practices are ethically, politically, and legally problematic. Weber and Bowling (2008) advocate for criminologists to continue studying the interaction between selection, exclusion and control in order to achieve a greater understanding of the social construction of difference. While not a focus of the current study, the concept of racial discrimination should also be explored in future studies examining the risk assessment process to expand on the works of O'Malley, Weber and Bowling. The

above-mentioned themes bring forth an important research question that the current study will examine:

Research Question 3: Do personal vulnerabilities such as previous discrimination and/or anxiety towards expert systems of technology contribute to people's concern about the possible discriminatory consequences of biometric passports in the risk society?

O'Malley (2006) argues that the process of discerning between high risk and low risk travelers attempting to cross international borders is discriminatory as risk assessments are largely based on components of racial profiling. Individuals who resemble the profile of previous terrorists are targeted for extended questioning while those who do not pass through security without question. With few details available regarding the specifications of the biometric passport that will be issued in 2011, it is difficult to anticipate potential discriminatory consequences. However, since biometric passports will have to be standardized to facilitate international travel many of the potential consequences of the Canadian biometric passport have already been realized in other countries. Biometric technologies may reveal certain ethnic and health features that an individual may not want to divulge including AIDS and diabetes (Liberatore, 2007). Biometric technologies are also discriminatory towards people whose religious views prohibit them from submitting biometric data [1] and/or people with disabilities as these people may not be able to submit for biometric testing. Therefore, the current study hypothesized that individuals who have experienced discrimination in the past may be more likely to anticipate problems of discrimination associated with biometric technologies.

---

[1] For some, biometrics are considered the mark of the Beast because Revelation 13:16-18 in the Bible states: "He also forced everyone, small and great, rich and poor, free and slave, to receive a mark on his right hand or on his forehead, so that no one could buy or sell unless he had the mark, which is the name of the beast or the number of his name."

It was also hypothesized that individuals with a high level of anxiety towards experts would be more likely to possess a general distrust for expert systems of technology. Anxiety induces suspicion which creates fear towards technologies used to screen travelers as people may feel criminal when they are asked to provide fingerprints and are concerned with the possible manipulation and misuse of biometric data (Liberatore, 2007). These concerns may evoke uncertainties regarding the processes behind the security measures and the risks associated with the technologies including discrimination and exclusion.

In sum, there is an increasing awareness in society regarding risk and insecurity created by science, technology, and globalization. This awareness heightens the need to identify and monitor these risks in order to effectively manage them. The various and competing definitions of risk and how it relates to danger and threat will affect the way people perceive risk and the subsequent need for security (Ekberg, 2007). Reflexive modernity is concerned with the individualized responses to uncertainty and the consequences of continuous monitoring and managing of risks (Ekberg, 2007). With the use of surveillance and biometrics an individual can expect to be constantly monitored outside of his or her home. The continuous use of these technologies is arguably a form of social control (Lyon, 2005), and an infringement of privacy rights (Solove, 2006). However, biometric identification technologies are also touted as being very efficient systems of identification (Reid, 2004; & Wayman, Jain, Maltoni, & Maoi, 2005). This lack of consensus among experts brings forth a great deal of tension between trust and skepticism towards expert systems for managing risk.

From the risk society perspective the increase of risk definitions (Ekberg, 2007) and the increasing awareness of risk results in the omnipresence of risk (Garland, 2003). Following this premise it could be argued that people are increasingly willing to accept the use of expert

technologies to manage these increasingly incalculable risks. Van Loon (2000), Giddens (1996) and Ekberg (2007), among others, have highlighted the contradiction between the increasing reliance on experts to measure and manage risks while the method of science is increasingly being delegitimatized due to its perceived failure to effectively manage these risks. However, an important aspect of risk in contemporary society is not only the increase in awareness of risk but also the new forms of risk now prevalent due to advances in communication, information and transportation technologies. While skepticism and distrust towards experts and expert systems of identification still exist, the proliferation of such systems has continued in the network society as more efficient ways to store and disseminate information is sought. As such, a discussion of the network society follows, from which research questions regarding the normalization of extraordinary technologies were drawn.

2.1.2 The Network Society

Technological solutions that operate within a networked society are increasingly sought to manage the risks and uncertain situations that plagued contemporary society. These expert systems of technology are often touted as efficient methods to identify people however; this efficiency highlights the omnipresence of risk and the potential for technological solutions to create even more risks. Therefore, the network society and the operation of technologies within the network are discussed below.

The social structures that characterize the network society are operated by information and communication technologies capable of processing and distributing information based on the knowledge accumulated in the nodes of the network (Castells, 2006). The social structures of the network society include the organizational institutions of human interaction that are capable of expression by coded communication such as institutions of production, consumption,

reproduction and power (Castells, 2004). A network therefore, works as a set of interconnected nodes where a node is defined by the type of network (Castells, 2000). Within the Information Age, for example, TV systems, entertainment studios, media crews, and mobile devices are nodes within the global network of news media (Castells, 2000). Flows are streams of information that travel between nodes characterized as "purposeful, repetitive, programmable sequences of exchange and interaction between physically disjointed positions held by social actors in economic, political, and symbolic structures of society" (Castells, 2000, p.442). Castells argues that society is structured around flows of technology, information, capital, interaction, images and sounds (Castells, 2000). The global networks of finance, communication, information, technology, and culture shape human interaction worldwide. However, these networks operate on a binary logic of inclusion/exclusion (Castells, 2004) whereby those without access to the networks are divided and marginalized (Castells, 2001). The distance between nodes in a network is zero whereas the distance between a node in the network to a node outside the network is infinite unless the program of the network is changed to enable the node outside the network to gain access to the network (Castells, 2004). The distribution of information and communication technologies is highly uneven and these technologies alone cannot solve social problems. Castells (1999) however, argues that advances in these types of technologies are not only a pre-requisite for economic growth but also for social development worldwide.

Production and accumulation are acclaimed under capitalism while communication and circulation are considered privileges in the network society (Lash, 2002). In today's technologically developed network society, information gathering has become a predominant strategy for managing goods, people, and information. Biology, electronics, and information are increasingly interacting and converging in their materials, application and conceptual approach

within this information technological revolution (Castells, 2000). This technological transformation is characterized "by its ability to create an interface between technological fields through common digital language in which information is generated, stored, retrieved, processed, and transmitted" (Castells, 2000, p.29). The network society is composed of systems that have the capacity to translate all inputs into a common information system. The electronic passport reader, for example, is a powerful tool that is able to process information quickly within an omnipresent retrieval and distribution network.

According to Castells networks are more than just an efficient way to organize information; they are also a sign of a new era (Stalder, 2006). Networks are increasingly becoming the dominant method of organizing all aspects of social life (Stalder, 2006). Contemporary networks scale far better than previous networks as they are no longer restricted by the complexities of their internal coordination (Stalder, 2006).

> ... they [have] become the most powerful form for organizing instrumentality... The strength of networks is their flexibility, their decentralizing capacity, their variable geometry.... their fundamental weakness, throughout history, has been the difficulty of co-ordination towards a common objective, toward a focused purpose, that requires concentration of resources in space and time within large organizations, like armies, bureaucracies, large factories, vertically organized corporations. With new information and communication technology, the network is, at the same time, centralized and decentralized. It can be co-ordinated without a centre (Castells, 1999, p.6).

The flexibility, scalability, and survivability of networks contribute to its efficient organizational capabilities as current communication technologies are capable of processing more information in less time and across larger spaces than ever before (Stalder, 2006). The flexibility and horizontal communication afforded by informational networks enables large-scale interaction and coordination amongst various social actors (Stalder, 2006). A discussion about border security follows as an empirical example of this concept.

Electronic information flows facilitate travel through borders as borders represent an interesting case of entry into the social contract. Entry into another country is not inherited or afforded by rights but rather a status that must be requested and assessed at the border (Salter, 2006). A 'state of exception' exists at the border as travelers are subjected to increased security screening and laws determining their eligibility to pass through borders yet are unable to claim mobility rights as the decision to grant access is determined by an agent of the sovereign who is concerned with national security (Salter, 2006). Certain legal rights are suspended at the border in the name of public security subjecting travelers to extensive searches and questioning (O'Malley, 2006). Searches and interrogations conducted at the border are deemed reasonable simply because they are carried out at the border pursuant to the right of the sovereign to protect itself and subsequently its inhabitants (Salter, 2006). The decision to grant or deny entry ultimately rests with the sovereign state through which the essence of state sovereignty is thus the monopoly to decide (Salter, 2006). Border officers (agents of the sovereign), classify travelers as national, stateless, refugee, foreign or alien and have absolute power to decide who crosses the border and who does not (Salter, 2006). In this particular space of decision and space of exception the individual traveler does not even possess his/her nationality unless one of the agents of the sovereign verifies and accepts it. Travel documents, border officers, surveillance technologies, and any other information provided by an agent, database, or institution during a background check all operate within a network designed to ensure proper identification to enhance security. Therefore, Canada's approach to national security emphasizes Canada as both a sovereign state concerned with ends-means strategies and as a united population subjected to increasing regulatory mechanisms in the name of security (Bell, 2005).

Within the network society information and communication technologies are increasingly sought to manage flows of people traveling through borders. Technologies that were previously used on welfare recipients, immigrants, or as pilot programs are increasingly broadening their scope thus extending surveillance technologies to the entire population (Ceyhan, 2006). After the attacks of 9/11 government and law enforcement officials in the United States increasingly sought out new methods of identification to "securitize identities and identification means and to monitor the movements of people inside and across borders" (Ceyhan, 2006, p.109). Identification technologies such as biometric systems operate as interrelated systems that collect, process, and disseminate information with the objective of providing a very high standard of proof of identity (Ceyhan, 2006). The integration of these identification technologies, according to Ceyhan (2006), is premised upon the interaction of three basic logics. The first of these logics is the logic of security concerned with the identification and interception of risks and risky people (Ceyhan, 2006). The second is a logic of management concerned with managing flows of people, goods, and transportation (Ceyhan, 2006). The third logic, ambient logic, relates to the integration of expert technologies into the everyday lives of individuals to familiarize people with the technology (Ceyhan, 2006). Within the network society, identification technologies are capable of permeating various societal spheres assisting law enforcement officials with identification at ports of entry (biometric passports) and extending into the domestic sphere (finger scans on laptops) where these exceptional technologies become normalized and a part of our everyday lives. This particular theme relating to the integration and normalization of extraordinary technologies into the everyday lives of individuals brings forth an interesting research question about people's preferred biometric identifier.

Research Question 4: Has the normalization of extraordinary technologies garnered greater support for facial scanning technologies or is finger scanning the preferred method of biometric identification?

The use of fingerprint technology dates back to the 18th century and is one of the most commonly used biometric technologies to date (Privacy and Technologies of identity, 2006). Fingerprinting is becoming cheaper, easier to implement and is gaining popularity in protecting personal property such as laptops and cell phones (Privacy and Technologies of identity, 2006). However, an individual's most visible feature is his/her face; therefore it is no surprise that facial scanning is becoming increasingly popular and expanding into commercial and domestic spheres as well (Cehyan, 2006). The increasing popularity of sci-fi movies and facial scanning systems used in other parts of the world has facilitated the integration of biometric technologies into daily life, which may make users more comfortable with and more accepting of biometric technologies for identification purposes (Liberatore, 2007).

In the network society perspective, Castells highlights the tension between the dynamics of global networks of economic, cultural and political relationships, and the particularities of local identities as the fundamental tension within network society (Stalder, 2006). Advances in technology have enabled the creation of databases and networks capable of generating, storing, retrieving, processing and transmitting large amounts of data (Castells, 2000). In a society of increasingly global networks, risks associated with a breach of the system must be managed to protect the information of countries and individuals in the databases. Governments must therefore manage the competing interests of increasing the securitization of borders while sustaining global economic flows (Weber & Bowling, 2008). Concepts and themes from the network society theory will be used to update the risk literature by examining the relationship

between biology, electronics, and information that is transferred through global distribution networks and how this impacts individuals' perceptions of risk and the normalization of extraordinary technologies for managing these risks.

After having situated the current study within a theoretical context it now becomes important to discuss biometric technologies generally and passports more specifically in order to provide an overview of the empirical issue currently under study. An examination of the various biometric technologies considered for use on biometric passports is provided below followed by a discussion of the importance of the passport as an identification document.

2.2 **Background Information**

2.2.1 Biometric Technologies

The International Civil Aviation Organization and the European Commission recommend the use of facial scans as primary biometric identifiers on passports and the use of finger scans as secondary identifiers, if necessary (Liberatore, 2007). Therefore, the following sections describe finger and facial scanning as the two main biometric technologies most commonly recommended and used on passports. The first section describes what biometrics are and how biometric systems operate. The next two sections discuss finger and facial scanning, their usage as well as their associated advantages and disadvantages. The final section of this chapter examines the passport as an identification document.

A biometric is a physical trait or behavourial characteristic that can be measured, recorded and ultimately quantified (Reid, 2004; Woodward, Orlans, & Higgins, 2003). Examples of physical traits include hand geometry, fingerprints, irises, retinas and faces; while behavioral characteristics include signatures, voice, keystroke and gait (Wayman et al., 2005). Biometric technologies employ automated methods to identify or authenticate the identity of a person based

on their physical traits and behavioural characteristics (Wayman et al., 2005). A biometric identification system is designed to test one of two possible scenarios: that the biometric data provided by the user is (1) not known to the system or (2) is known to the system (Wayman et al., 2005). Methods of identification and authentication are utilized to facilitate the determination of identity and authorized access. The process of identification employs a 'one-to-many' (1:N) matching method whereby an individual's biometric data is compared to all biometric data on file (Fumy & Sauerbrey, 2006; Reid, 2004). One-to-many matching is often used in law enforcement where biometric data is compared to data previously stored in the database (Reid, 2004). The system compiles a list of possible matches at which time human intervention is required to determine whether a positive match exists within the system. Biometric systems are also able to employ authentication methods whereby a user presents his/her biometric data to be compared and authenticated against that user's biometric data previously stored in the system (Reid, 2004). This process is referred to as 'one-to-one' (1:1) matching whereby the response generated is simply 'yes, the individual's identity is authenticated or 'no, the individual's identity could not be authenticated'. This type of matching is often used to grant or deny access to specific areas (Fumy & Sauerbrey, 2006; Reid, 2004).

Biometrics can be classified according to the level of subject involvement. Passive biometrics do not require active participation from the subject as these systems are typically covert (Reid, 2004 &Woodward, 1998). Face, voice and gait can all be measured without the subject submitting to the measurement (Reid, 2004; & Woodward, 1998). Passive biometric systems generally use identification methods to compile a list of possible matches stored in the system for use by a human operator who determines the validity of the match (Reid, 2004). Passive biometrics are commonly used in surveillance applications and are often seen as a breach

of privacy (Reid, 2004). Alternatively, active biometrics require the active participation of the subject and are considered overt and less of a threat to privacy (Reid, 2004 & Woodward, 1998). Examples of active biometrics include hand geometry, fingerprinting, and retina and iris scanning (Wayman et al., 2005). Active biometrics are often used to authenticate a subject's identity. This process involves the subject making a claim as to who he/she is, supplying some form of ID, and then providing biometric data for comparison (Reid, 2004; &Woodward, 1998).

Finger and facial scanning, individually or combined, could be used as unique identifiers on biometric passports and are either well established or are gaining popularity. According to Reid (2004) a good biometric is defined in terms of: user acceptance, ease of use, cost, deployability, invasiveness, and the time it takes a user to become habituated. These and other aspects of finger and facial scanning identification technologies are discussed below.

2.2.2 Fingerprint Identification Technology

There are a plethora of reasons why fingerprint technology is one of the most popular methods of identification in the biometric market today. One is because fingerprints have a long, established history as over 100 years of knowledge has accumulated on the origin, development and uniqueness of fingerprints (Wayman et al., 2005). Sir Edward Henry's book *Classification and Uses of Finger Prints,* written in 1900, describes the first robust fingerprint identification system, the foundation of which is still used in today's fingerprint classification systems (Reid, 2004; & Woodward, Orlans, & Higgins, 2003). Fingerprints are described and ultimately identified by the ridges (elevations) and valleys (depressions) that form unique patterns (Reid, 2004). These individualizing patterns are why fingerprints have a high discrimination rate and subsequently why they are used for large-scale identification purposes (Hribernig & Weinzierl,

2006; & Reid, 2004). Scientific qualifications regarding the amount of discriminatory information present in fingerprints have effectively demonstrated the validity of fingerprints for many diverse identification functions (Wayman et al., 2005). Fingerprint identification technologies can be deployed in a variety of environments for a multitude of purposes. For example in 1903, in the New York state prison, fingerprints were used for the identification of criminals (NSTC, 2006). In 1999 the FBI deployed IAFIS (the Integrated Automated Fingerprint Identification System) a national network for electronic fingerprint submission, which enabled criminal background checks and the identification of prints found at crime scenes (NSTC, 2006). Finger-scan readers, like the ones implemented at The Royal Grammar School in Surrey, UK to control access to rooms that had previously been stolen from, are used in schools to monitor registration, attendance, library use, and meal options (Spence, 2000). Today, finger scans are increasingly used to gain access to cell phones and laptops and to gain entry into restricted areas.

2.2.3 Advantages of Fingerprint Technologies

Fingerprint technology has many advantages for law enforcement officials, some of which arise from its basic technology, while others stem from the needs of the biometric marketplace (Nanavati, Thieme & Nanavati, 2002). Fingerprint technologies are considered highly distinctive identifying methods capable of processing a large number of people with a high level of accuracy (Nanavati, Thieme & Nanavati, 2002). While iris and retina scanning use more physiologically distinct characteristics for identification, champions of fingerprint technology have touted the long history of the use of fingerprinting (decades not years) to uniquely identify individuals (Nanavati, Thieme & Nanavati, 2002). The use of fingerprint scans for identification purposes is already wide spread throughout the biometric marketplace which

leads proponents of the technology to believe that it will be accepted for identification purposes on electronic passports.

The biometric marketplace is increasingly becoming dominated by fingerprint technologies as these easy-to-use devices can be deployed in a wide-range of environments (Nanavati, Thieme & Nanavati, 2002). Unlike facial and iris scanning, fingerprint technologies are resistant to changes in the environment such as temperature and lighting (Nanavati, Thieme & Nanavati, 2002). This particular advantage is especially important for law enforcement officials as the identification of travelers occurs in various environments at borders throughout the world. Furthermore, unlike some biometric technologies that require extensive user involvement, fingerprint technologies are relatively easy to use as the new devices guide the finger into proper placement (Nanavati, Thieme & Nanavati, 2002). This versatility coupled with the decreasing cost and size of the devices has made fingerprint technology the dominant method of identification for logical and physical access control (Nanavati, Thieme & Nanavati, 2002). Outside of law enforcement, the ease of use of finger scan technologies has helped finger scans gain popularity for securing laptops, cell phones, workplaces, and restricted areas. The use of finger scan technology in routine activities helps familiarize users with the technology possibly to the point where they will accept the use of fingerprint identification technologies in combination with electronic passports.

From a law enforcement perspective, ensuring the safety of travelers and citizens of traveled countries is of paramount importance. In order to enhance security, some fingerprint identification systems allow users to enroll multiple fingers which reduces the false match rate as the odds of falsely matching two fingers is astronomical (Nanavati, Thieme & Nanavati, 2002). Biometric passports printed in Germany after November 2007 contained two fingerprint scans,

one from each hand (European Digital Rights, 2005) which serves to decrease false match rates and to increase security by reducing the possibility of stolen fingerprints being incorrectly verified (Reid, 2004). Fingerprint devices can also be programmed to challenge the user to put forth one of several fingers for scanning or input a sequence of fingerprints in the proper order (Reid, 2004). This type of security would make identity theft extremely difficult as the potential thief would need to know which fingers to present for scanning and/or in which order.

2.2.4 Disadvantages of Fingerprint Technologies

Scientifically, fingerprints have proven to be valid methods of identification. However, they are also associated with criminal investigations and as such may not receive complete acceptance from the public. Having to provide a fingerprint to prove one's identity is an involuntary invasion of privacy and somewhat of a reversal of the notion of innocent until proven guilty (Liberatore, 2007). Citizens may feel as though they are being treated as 'suspects' who then have to prove their innocence or in this case, identity. The involuntary nature of biometric data submission has privacy advocates apprehensive about biometric data collected for a specific purpose and the possibility of function creep. Function creep occurs when data is used for a purpose other than for what it was originally collected; for example, when biometric information is used to track people's activities (Liberatore, 2007). Function creep becomes even more of an issue when biometric data is shared across departments and throughout various agencies. Fingerprint technology's association with criminal investigations and its potential to invade one's privacy may inhibit the growth of fingerprint identification systems for various applications. However, with regards to biometric passports, fingerprints may seem less invasive than facial scanning (Nanavati, Thieme & Nanavati, 2002).

Like any biometric there is a small percentage of the population that are unable to enroll in the biometric system, an obvious problem for law enforcement officials attempting to verify the identity of travelers crossing international borders (Nanavati, Thieme & Nanavati, 2002). For fingerprint biometrics up to 5% of any given population cannot enroll (Reid, 2004). Studies have shown that manual labourers, elderly people, as well as some Asian people, often have lower quality fingerprints and are therefore less likely to be able to enroll in a fingerprint system (Nanavati, Thieme & Nanavati, 2002). Psychological reasons, including feelings of criminality and religious beliefs[2], also present a challenge for enrollment and the use of fingerprint technologies (Reid, 2004). This would mean it would be necessary to have an alternative identification system to identify those unable to enroll in a fingerprint identification system. For biometric passports, an alternative system would detract from the advantages of using biometric passports mainly efficiency and security.

2.2.5 Facial-Scanning Technology

The question of whether a computer can read a face as well as a human being dates back to machine vision research conducted in the 1970s (Woodward, Orlans, & Higgins, 2003). Humans are able to quickly and easily recognize hundreds of faces from their friends and family members to public and celebrity figures based on familiarity and uniqueness of facial features (Woodward, Orlans, & Higgins, 2003). Computers however, use a much more calculative approach to verify or identify faces and facial features (Nanavati, Thieme & Nanavati, 2002). One's face consists of macro features such as the mouth, nose, eyes, cheekbones, ears, lips, chin, and forehead as well as micro features such as the distance between the macro features or the specific size of a feature itself (Reid, 2004). Facial scanning technology is used to acquire an

[2] Religious beliefs that prohibit them from submitting biometric data.

image of a face, process the image, locate distinct characteristics, create a template and then match that template to an enrolled template (Nanavati, Thieme & Nanavati, 2002).

During the 1960s and the 1970s scientists were concentrated on developing facial recognition technologies with automated capabilities. In 1988 the first semi-automated facial recognition system was deployed at the Lakewood department of the Los Angeles County Sheriff's Department where video images of a suspect's face were compared to digitized mug shots contained in a database. In 1991, the discovery of real time facial recognition technologies led to increasing interest in the technology for identification purposes. During the 2001 Super Bowl in Tampa, Florida, facial recognition was used to scan the crowd and identify any 'wanted' individuals attempting to enter the stadium (Fleming, 2003). More recently, a 'wanted person' facial recognition system has been implemented in the United Arab Emirates (UAE). Initially airport based, this system has now been expanded to all ports of entry in the UAE (Face Recognition, 2008). Furthermore, convenience stores in the UK are implementing *Age Watch*, a program that uses facial scanning technologies at the point of sale to capture and compare the face of a customer to a database of profiles containing a list of minors who previously attempted to purchase alcohol and/or tobacco while under age (Face Recognition, 2008). More commonly, facial recognition technologies are used to gain access to items of personal property such as laptops and/or to gain entry into restricted areas (Face Recognition, 2008). On a daily basis people recognize and verify other's identities based on the characteristics of their face (Reid, 2004) and as such, proponents of facial scanning technology argue for its acceptance based on the fact that facial recognition is the most natural way to identify humans (Hribernig, & Weinzierl, 2006). This relative familiarity may offer a level of comfort and ease to individuals weary of facial scanning technologies.

2.2.6 Advantages of Facial Scanning Technologies

From a policing perspective, a significant advantage of using facial scanning techniques for identification purposes is that facial scanning is a software based technology that can utilize imaging systems already in place (Nanavati, Thieme & Nanavati, 2002). Standard video cameras, CCTV cameras and photo identification systems are widely used and are able to support facial scanning technology without the need for new equipment. The benefits afforded by this, namely, cost efficiency and ease of implementation, help keep facial scanning technology a competitor in the biometric marketplace. (Nanavati, Thieme & Nanavati, 2002).

From a law enforcement perspective, the ability for facial scanning technologies to identify subjects without their knowledge or consent is an attractive feature for surveillance purposes (Nanavati, Thieme & Nanavati, 2002). Casinos have adopted this technology into their current monitoring systems to facilitate the identification of suspicious persons (Nanavati, Thieme & Nanavati, 2002). The mandated use of biometric passports will ultimately lead to the creation of a database that contains all users' submitted biometric data. This database could be used to match the face of a subject under surveillance to his/her enrolled biometric data.

The ability of facial scanning to enroll static images is also an attractive feature to law enforcement officials concerned about the time it takes to enroll users in a large-scale biometric system (Nanavati, Thieme & Nanavati, 2002). Many large-scale systems take three to five years to enroll the target population. However, images collected in existing databases (such as immigration offices and transportation ministries) can easily be added into an identification system that employs facial scanning software (Nanavati, Thieme & Nanavati, 2002). This advantage however, would be inapplicable for biometric passports as users would still need to go

through the process of obtaining and subsequently renewing their passport which would require a new photo to be submitted every X number of years.

2.2.7 Disadvantages of Facial Scanning Technologies

From both a policing perspective and a citizen's point of view, one of the most important features of an identification system used at border crossings is the system's accuracy. Facial scanning technologies operate most effectively when enrollment and verification occur under the same conditions (Nanavati, Thieme & Nanavati, 2002). Background lighting, temperature, camera quality and positioning, as well as the angle from which the picture was taken are various factors that can dramatically affect the accuracy of the system (Nanavati, Thieme & Nanavati, 2002). Therefore, environmental conditions would need to be standardized at passport offices and border crossings to reduce the effects of background conditions.

Changes in physiological characteristics over time can also affect the accuracy of identification systems. Critics of facial scanning technologies have highlighted the effects of how simple modifications such as changes in make-up, facial hair and the removal of eyeglasses can cause users to inaccurately be rejected (Nanavati, Thieme & Nanavati, 2002). Other, more challenging, issues arise when dealing with identical twins and people who have had plastic surgery. Proponents of facial scanning technology counter by highlighting the constant advancements of the technology and are confident that this technology will be able to overcome these challenges in the near future (Nanavati, Thieme & Nanavati, 2002). However, even with an extremely high success rate the number of false positives that would be identified would be unacceptable. Cited in the article *A world away from reality* by David Birch published in *The Guardian*, is the example of London's Heathrow Airport which processes over a million

travelers every week. Even if facial scanning had a 99.9% accuracy rate the technology would incorrectly verify or reject over a hundred passengers each day (Birch, 2002). Not only would this inconvenience the innocent travelers who would be subjected to increased security screening but it would also diminish airport security's trust in the reliability of the technology to accurately identify passengers which could cause them to disregard the warning of a suspected traveler in the future. Birch (2002) argues that "as with CCTV in town centres, the cameras might make us feel safer, but they wouldn't necessarily make us safer" (Birch, 2002, Technology news & features section, p.2).

While the accuracy of identification systems is essential for law enforcement officials as well as citizens, privacy advocates and citizens alike are fearful that the biometric data submitted by the user for passport identification purposes could be used to track individuals (Nanavati, Thieme & Nanavati, 2002). Other biometric identifiers face the same issue; however, in most cases, it is easier to track a person using an image of what they look like than to track someone using their fingerprints, as cameras are present in most public places. Within the risk society it is presumed that, to a certain extent, people are willing to give up a certain degree of personal privacy for a collective gain of enhanced security. However, it is becoming increasingly difficult to balance the rights of individuals with the security of the whole as risks are becoming more evident with constant surveillance in the risk society.

While biometric identification systems can be extremely efficient methods of managing flows of people, the problems that can occur during enrolment, verification, storage, retrieval and transmission cannot be ignored. False positives (an individual is mistakenly verified as someone else), false negatives (an individual is not recognized by the system), function creep (data used for improper purpose), and discrimination/exclusion (certain ethnic and health issues can be

exposed through biometrics) are some of the main issues that will need to be addressed in order for users to accept the use of biometric technologies and for the technology to perform at its best.

It is evident in the preceding sections that both finger and facial scanning have advantages that make them attractive as methods of identification. However, more research into the disadvantages of each of the biometrics is needed before the implementation of biometric passports in Canada in 2011. An accurate and efficient travel document is vital in order to securitize borders while enabling global travel therefore, an examination of the passport, which is provided to give contextual relevance to the importance of effective identification documents and systems of identification, follows.

2.2.8 Passports

According to John Torpey (2001), the modern state is the result of three interrelated processes: 1) the monopolization of the legitimate use of violence and the establishment of a supervisory control of subject populations, 2) the establishment of clear-cut borders and the management of the movements of people inside the territory and at the borders, and 3) the establishment of a monopoly over the identification of individuals by the issuance of documents, such as a passport or an ID card. Torpey (2000) also highlights the critical role played by passports in modern states and posits that passport documents have been crucial in terms of state-building. Passports allow for the identification of membership and the verification of the legitimacy of claims to the rights and benefits of this membership. Torpey (2000) posits that passports serve as a mechanism of state control as the state has essentially expropriated and monopolized the legitimate means of movement by affirming control over bounded territories and individuals' freedom to move across jurisdictional spaces. Passports are, however, valuable

documents in terms of citizenship and identity as they entitle the bearer to certain privileges including legal protection while abroad and the right to re-enter one's country of nationality.

Biopower and sovereign power constitute liberal practices of government and modern security strategies. According to Foucault (as cited in Bell, 2005), Western societies have been marked by biopower since the seventeenth century whereby power over man insofar as man is a living being, signified the materialization of state control over biological life. This essentially enables the elimination of weaknesses that threaten the sovereign and/or the people of the territory (Bell, 2005). Security of life therefore, increasingly becomes concerned with identifying risks that threaten the whole. The protection of the territory and the population as a whole is therefore of paramount importance. Terrorism and other threats to national security are thus taken very seriously. Monitoring, managing, and when necessary, restricting, the movement across borders is imperative to the security and protection of the nation state. The passport plays an increasingly important role in this process as it enables global travel while protecting the nation state.

Accurately determining the identification of individuals has become increasingly difficult and as such, various methods of identification have been tested for efficiency and accuracy. Biometric scanning for identification purposes has become increasingly popular in various domains of society throughout the world. Biometric scanning is used in law enforcement, prison management, the military, national security, border control, licensing, entitlement programs, and identity cards (Woodward, 1998). The collection of biometric data has also enabled the creation of sophisticated identification documents including national ID cards and electronic passports. The electronic passport issued in the United States contains an integrated circuit computer chip that stores a digital photograph and the same information visually displayed on the regular photo

page of the passport (name, birth date, gender, birth place, dates of passport issuance and expiration, and passport number). Facial recognition technologies are used at international borders to compare and verify the digital photo on the passport (Bureau of Consular Affairs, 2007). Mechanisms of identification serve various purposes. National ID cards and electronic passports however, are generally used by authorities to identify people who are citizens of a particular nation state (Lyon, 2005). The ability to quickly and automatically distinguish between citizens and non-citizens greatly increases the surveillance capabilities of the nation state, which in turn facilitates the management of that state and its people (Lyon, 2005). This type of surveillance brings forth civil liberty issues including the freedom of movement and has been implicated as a social sorting technique (Lyon, 2005). The implementation of biometric identification cards highlights the shift from an identification process based on discretion and compassion to an automated classification system. Surveillance within this type of electronic infrastructure is concerned with personal data for the purpose of influence, management or control (Lyon, 2005). The passport however, is an important element of the policies and procedures set forth to identify the national population in order to protect the border (Torpey, 2001). The passport has emerged as the primary document of identification for international travel as it uniquely identifies the traveler, his/her point of origin, and the state to which he/she can be deported to if necessary (Salter, 2003).

In the search for terrorists after 9/11, national security has become increasingly more important than ensuring the rights of innocent citizens (Pomerance, 2005). The importance of identification documents for traveling and maintaining national security is evident. The proposed enhancement of border security via biometric passports has brought forth various issues that civil libertarians and privacy conscious individuals are concerned about (Ng-Kruelle et al., 2006). A

study examining user's acceptance of e-Passports in the European Union identified the invasion of privacy as the most prevalent area of concern among negative respondents (Ng-Kruelle et al., 2006). Travelers may be willing to give up some personal privacy and accept the use of biometric passports for national security; however, they would want to ensure that their personal biometric data is safely stored and protected in a database.

Simultaneously securing individual rights and protecting national security is a difficult task to accomplish. Experts and marketers of the technology are confident that biometric technology is capable of advancing in a manner that will potentially create more of a balance between the two functions. The methods of identification may have changed but the function of the passport has not. Therefore it is imperative for privacy advocates and citizens alike to continue to challenge technology and the mechanisms that back their usage in order to drive the technological advancements that are necessary to obtain such a balance.

The need for effective methods of identification is apparent however; there is a lack of consensus among experts regarding which system of identification would provide the highest level of security while ensuring the rights of individual citizens. The current study employs a fairly unique methodological approach by probing the perceptions of future users of biometric passports before their issuance in 2011. What follows is a summary of the research questions highlighted throughout the literature review of the current paper as well as the methodological decisions employed in the current study.

2.2.9 List of Research Questions

Before discussing the methodology of the current study, a list of the research questions derived from the literature review examined above, is provided below in order to gain a greater understanding of the study as a whole.

- *Research Question 1*: In what types of situations are people willing to provide biometric data for identification purposes during a time when science and expert authority is being questioned in the risk society?
- *Research Question 2:* Do individual characteristics such as frequency of travel, familiarity with biometrics, anxiety towards expert systems, perceptions of safety or previous victimization contribute to the acceptance or non-acceptance of biometric passports in the risk society?
- *Research Question 3:* Do personal vulnerabilities such as previous discrimination and/or anxiety towards expert systems of technology contribute to people's concern about the possible discriminatory consequences of biometric passports in the risk society?
- *Research Question 4*: Has the normalization of extraordinary technologies garnered greater support for facial scanning technologies or is finger scanning the preferred method of biometric identification?

Ekberg's conceptual model (discussed at length above) identified six unique parameters of the risk society which helped guide the current study as well as some of its research questions. The technical, virtual and manufactured risks prevalent in the risk society create security situations unknown to previous generations. Technological advancements have enabled greater

risk detection however; these devices also highlight the prevalence of risk and the expanding definitions of risk. With the collapse of traditional norms and group belonging for guidance, individuals are forced to trust expert systems of technology to manage the increasingly incalculable situations of the risk society (Ekberg, 2007). These parameters of the risk society brought forth important elements for discussion and examination, including the paradox highlighted by Van Loon (2000) regarding the increasing role of scientific expertise as science itself suffers severe criticism, which ultimately lead to research question number one which asked 'In what types of situations are people willing to provide biometric data for identification purposes during a time when science and expert authority is being questioned in the risk society?' With this particular research question the current study attempts to gain a greater understanding of the domains in which these technologies have become integrated into. This research question also has the potential to probe into the hypothesized ambivalent relationship people have towards science and technology by examining which of the various uses of biometric technologies people are accepting of.

The relationship between risk and trust is one of the parameters identified in Ekberg's conceptual model that the current study examined more closely. Within the risk society trust takes on a new significance, as trust is no longer embedded in kinship or religion but rather in faceless commitments such as money and expert systems (Ekberg, 2007). According to Ekberg, a major contention within the risk society is the trust/skepticism dichotomy. Expert systems of technology are increasingly used to manage risks but science is no longer considered infallible or the only source of truth (Giddens, 1996). Therefore, research question number two of the current study was created to examine if individual characteristics such as anxiety towards expert systems, perceptions of safety, previous victimization, familiarity with biometrics or frequency

of travel contributed to people's acceptance of biometric passports. This particular research question will expand the current knowledge around the hypothesized ambivalent relationship people have towards science and technology highlighted by Van Loon (2000) by examining whether or not negative perceptions of safety (Nugent & Van Daele, 2006), fear of crime (Leiker, 2006), and/or anxiety towards expert systems (Liberatore, 2007), are associated with people's acceptance of heightened security measures such as biometric passports.

Further research into the areas of border security and risk management highlights some of the potential discriminatory implications of biometric methods of identification. The basic element of border security is discriminating between desirable and undesirable travelers (Salter, 2004). However, within a risk-based approach to border security our ability to identify and manage uncertain events is inherently limited (Garland, 2003). According to O'Malley (2006), the process of discerning between low-risk and high-risk travelers stems from elements of profiling which is a cyclical process whereby predictive risk assessment tools reproduce the data they were based upon, reaffirming the reason for targeting those particular individuals. Furthermore, O'Malley (2006) asserts that these risk prediction tools are weak and are ethically and legally problematic. Moreover, David Lyon (2006) contends that discriminating between various travelers and subjecting them to differential treatment is essentially social sorting whereby members of a certain class are eligible for certain benefits while others are not.

Since Canada is not the first country to propose the implementation of biometric passports, some of the concerns surrounding their use have already been realized in other countries. Using this information, as well as the concerns voiced by proposed users of the passports, could help alleviate some of the problems associated with biometric passports prior to their implementation in Canada in 2011. This particular line of research led to the creation of research question

number three which asked 'do vulnerabilities such as previous discrimination or anxiety towards expert systems contribute to a person's concern about the possible discriminatory consequences of biometric passports in the risk society?' This research question was utilized to examine whether concerns about discrimination are general or specific to people who have been previously discriminated against or who have anxiety towards expert systems. This particular research question will also probe deeper into the hypothesized ambivalent relationship people have towards science and technology by examining people's concerns about discriminatory consequences of biometric passports and their associated levels of acceptance for these technologies despite their implications.

Many expert systems of technology, including biometric identification systems, are met with hesitation and skepticism among some members of the general public. Ceyhan (2006) highlights the importance of ambient intelligence whereby expert systems of technology are integrated into the daily lives of individuals to familiarize people with technological systems. Biometrics are increasingly used on identity cards, licenses, for entitlement programs, and to secure laptops, cell phones, and restricted areas (Woodward, 1998). Currently, the two main biometrics proposed for use on passports are facial scans and finger scans (Liberatore, 2007) which brought forth research question number four: 'has the normalization of extraordinary technologies garnered greater support for facial scanning or is finger scanning the preferred method of biometric identification?' While fingerprints have an established history of use dating back to the 18th century, they are associated with criminal investigations and as such, may not receive the acceptance that marketers of the technology had hoped for (Privacy and Technologies of identity, 2006). Conversely, while facial scanning technology is becoming increasingly popular in sci-fi movies, the technology is relatively new to the commercial and domestic

spheres and may therefore face resistance among members of the public. This particular research question will help identify the biometric identifier of choice among respondents as well as some of the reasons associated with the acceptance or non-acceptance of biometric passports. This research question will also shed light upon the varying degrees of integration achieved by both finger and facials scans and will also help expand the current knowledge regarding which particular technology, if any, people are ambivalent towards and potentially some of the reasons underlying this hypothesized ambivalence.

The research questions listed above were drawn from a comprehensive review of the literature pertaining to the nature of risk in contemporary society, safety and security post 9/11, the normalization of technologies, and the reliance on experts, among other themes. These research questions were investigated through the use of a student questionnaire, a discussion of this and other methodological decisions is below.

3 METHODOLOGY

3.1 **Research Design**

This study was conducted using non-experimental survey research within a cross sectional design. Non-experimental approaches study naturally occurring phenomenon without any intervention on the part of the researcher (Bachman, Ronet, & Schutt, 2003) while cross sectional research is conducted by collecting data from a sample at one point in time (Babbie & Benaquisto, 2002). Due to the nature of the study, feasibility, cost and time, the group-administered questionnaire used in this study was given to the study sample once. Based on the interdisciplinary nature of biometric technologies and border security a non-probabilistic purposive sampling frame was selected from the criminology, communications (media) and biology departments.

3.2 **Biometric Passport Implementation Questionnaire**

The creation of the Biometric Passport Implementation in Canada Questionnaire was guided by a comprehensive review of previous empirical and theoretical literature in the fields of criminology, sociology, as well as science and technology. The primary objective of the questionnaire was to gain a greater understanding of how English speaking students in first year courses at the University of Ottawa perceive the use of biometric technologies for use on passports in Canada and to expand the existing knowledge regarding the normalization of extraordinary technologies during a time when science is losing some of its dominant authority. The questionnaire assessed numerous variables including socio-demographic variables (age, sex, and race), variables about student status (level of education and program of study), acceptance variables (willingness to provide finger or facial scans for various purposes), as well as vulnerability variables (feelings of safety, previous victimization and discrimination).

3.3 Data Collection Procedures

Ethics approval for this research study was obtained from the Research Ethics Board at the University of Ottawa in August 2008 (See Appendix A). In November of 2008, department chairs from the Communications, Criminology and Biology departments were approached to obtain permission to conduct research in their respected departments after which time professors were approached to gain entry into classrooms to distribute the questionnaires during the 2009 Winter Semester. Questionnaires were distributed in classrooms with the researcher present to answer any questions the respondents had. Respondents were also given oral instructions regarding the questionnaire and were advised that participation was completely voluntary and anonymous. When participants were finished with the questionnaires they simply returned them to a box at the front of the classroom. A total of 370 questionnaires were distributed which resulted in 311 valid cases which represents a response rate of 84%.

3.4 Selection Criteria

English speaking individuals in first year courses whose professors granted the researcher permission were asked to participate in this research study. Cases were excluded if demographic information such as age, sex and race was not provided for analysis (n=8); or if the questionnaire responses seemed highly invalid (i.e. selecting every box on the survey [n=7]). Other inconsistencies in responses were also excluded from analysis (ie. answering 'No' regarding the support of facial scanning on passports and then responding that they support facial scanning on passports because it is convenient [n=11]).

3.5 Justification of Methodological Approach

Biometric passports are scheduled to be issued in Canada in 2011. While the details and specifics of these biometric passports have yet to be released it is important to conduct research prior to implementation in order to gain a greater understanding of how the mandated users of the passports perceive the passports as well as the technologies utilized by the passports.

3.5.1 Justification for Questionnaire

Survey research is a feasible way to obtain a large amount of information on a particular topic of interest (Babbie & Benaquisto, 2002). As a tool for the social scientist looking to gather original data from a large population, survey research is an excellent method for collecting a considerable amount of data in a short period of time. Furthermore, face-to-face contact with respondents yields relatively high response rates (80-90%) while questionnaires distributed to a group in a particular setting (such as a classroom) may even yield response rates closer to 100% (Palys & Atchison, 2008). Group-administered questionnaires within a classroom setting are economical and time efficient which gives a student researcher access to a large original sample for the purpose of data collection.

Survey research is particularly conducive to studying public perceptions and measuring attitudes in an anonymous forum (Babbie & Benaquisto, 2002). The questionnaire used in the current study collected no identifying information and all questionnaires (those completed and those left blank) were returned to a box in the classroom so it was not possible to determine which students filled out the questionnaire and which did not. The anonymity afforded by questionnaires allows individuals to freely express their attitudes and honest opinions privately without fear of identification.

Questionnaires specifically designed for a particular study, as oppose to secondary data, allow the researcher to ask the precise questions he/she wants responses to. Developing a questionnaire by utilizing the existing body of literature as a basis and expanding on specific areas of interest to the researcher allows for a greater understanding of the specific research questions currently under study.

One of the major advantages associated with survey research is that it enhances reliability. If another researcher wanted to replicate this study or test the results it would be possible to identify exactly what was asked of the participants as the questionnaire that was used in this study is provided as an appendix (See Appendix B). Furthermore, the questionnaire used in the current study was a structured questionnaire, which facilitates coding as well as replication.

Every type of research design has inherent problems as well as associated strengths. Survey research was selected because its advantages outweigh its disadvantages in terms of attempting to obtain a large amount of data from a population that is too large to directly observe. Surveying the mandated users of biometric passports prior to implementation is a fairly unique approach therefore it is necessary to collect a large amount of quantitative data to identify common themes and areas of resistance that need further, more specific exploration.

3.5.2 Justification for Study Sample

The sample population and location were chosen on the basis of feasibility and access. Given the researcher's resources and status as a student it would be difficult to obtain access to a large sample outside of the university setting. First year courses were selected for this study because first year courses would likely possess a more diverse study sample than upper level, more specialized courses would. Furthermore, within first year courses students will be in

different majors, as some will be taking the course as an elective. Additionally, students from upper year courses may be in a first year course (but not vice versa), which again provides more diversity for the study sample.

Another reason for choosing first year courses was to obtain a sample that was not significantly more educated than the general public so that the results of the study would not be restricted to a specific/specialized group but rather to a student-aged population. Surveying a student-aged population allows for the collection of information from the particular individuals who are growing up with this type of technology and who will be significantly impacted by the implementation of biometric passports.

3.6 **Limitations**

3.6.1 Limitations of the Questionnaire

The use of survey research also has various weaknesses that researchers need to be aware of. When constructing questionnaires it is important to ensure that the language used is appropriate for a range of respondents. Given the interdisciplinary and technical nature of the current study respondents were given an information letter and an oral statement that briefly described biometric passports and the purpose of the study. Furthermore, the questions on the questionnaire were written at a grade 9 reading level (as determined by the Flesch-Kincaid grade level score, a readability score test provided in Microsoft word). The researcher remained present throughout the duration of the questionnaire administration in order to answer any questions the respondents had.

Another limitation associated with structured questionnaires is that data collection is limited to the questions on the questionnaire. The researcher does not have the opportunity to ask any probing or follow-up questions. Therefore, questions must be clear and direct in order to

obtain a valid response to the question posed and to ensure the question is measuring what it is suppose to measure. Furthermore, with a structured questionnaire the questions asks are only approximate indicators of people's opinions as people's opinions rarely take the form of 'agree' or 'disagree'. On a closed-ended structured questionnaire there is no room for the respondent to elaborate or explain his/her response. Moreover, questionnaires cannot measure social action. Questionnaires are only capable of collecting self-reported data of recalled actions or future hypothetical action (Babbie & Benaquisto, 2002). This reliance on the participants' answers affects the validity of the study as there is no way to ensure that participants are answering the questions honestly; however, ensuring anonymity and confidentiality attempts to promote honest responses. The responses obtained by the questionnaire must therefore be taken at face value and reported as approximate indicators of people's perceptions regarding a particular topic.

3.6.2 Limitations of the Study Sample

External validity may pose a concern since only English speaking students in first year courses at the University of Ottawa were surveyed. In order to alleviate this problem, generalizations beyond this particular study will be limited. Furthermore, surveying students in first year courses (as opposed to more specialized courses) attempted to obtain a more diverse study sample. The majority of this particular study sample however, is relatively homogenous in terms of age and level of educational background.

3.7 **Measures**

This research study used SPSS version 16 for MAC as well as EXCEL 2004 for entering data and conducting analysis.

3.7.1 Demographics

Demographic information collected included sex, age, race, political party support, level of education, faculty of study, and religious affiliation. The demographic variables were collected in order to provide information about the respondents to see whether these factors returned significant differences in terms of acceptance for biometric passports.

3.7.2 Questionnaire Concepts

The following section outlines the questionnaire items that define the concepts used in the research questions of the current study.

Research question number two asks what 'individual characteristics' contribute to the acceptance of biometric passports. For the purpose of the current study, the term 'individual characteristics' was defined using the following questionnaire items:

- Frequency of travel outside of Canada: recorded as rarely (less than once in five years), annually, or two or more times a year.
- Familiarity with biometrics: low familiarity (coded as a score of 0-4 out of 16 on survey question number one), moderate familiarity (a score of 5-8 out of 16) or high familiarity (a score of 9 or more out of 16).
- Anxiety towards expert systems: includes questionnaire item number one which asked respondents if they trust iris, face, finger, or voice biometrics, as well as questionnaire question seven which asked respondents if they were concerned about a data breach or biometric data being used to track people.
- Perceptions of safety: includes questionnaire statements 8-13. The statements asked respondents what their perceptions were about whether Canada and the Canadian border were safe, if they felt that national security and individual rights were ensured, if they

thought terrorism in Canada was a threat and whether their local police were ensuring safety.

- Previous victimization: includes vandalism, theft, break and enter, motor vehicle theft or attempt, fraud, terrorism, assault, robbery, harassment, sexual assault and other. Coded as number of different instances of victimization.

Research question number two asks what types of personal vulnerabilities people possess that contribute to their concern about the possible discriminatory implications of biometric passports. For the purpose of the current study, the term 'personal vulnerabilities' includes:

- Previous discrimination: includes instances of discrimination based on age, gender, language, ethnicity, race, religion, sexual orientation, disability or other. Coded as the number of different types of discrimination experienced.
- Anxiety towards expert systems such as biometric passports: includes questionnaire item seven which asks respondents if they are concerned about data breaches or tracking as well as elements of questionnaire item one which asks if respondents trust facial and/or finger biometrics.

3.7.3 Victimization Index

An index is a composite measure that is composed of multiple indicators of the variable under study (Babbie, Halley, & Zaino, 2003). The COUNT command in SPSS was used to create The Victimization Index which is composed of the nine variables in questionnaire question # 14 which asked respondents to indicate which offences they had previously been a victim of: vandalism, theft of personal property, break & enter, motor vehicle theft/attempt, fraud, assault, robbery, harassment/stalking, and sexual assault. Respondents were coded into categories depending on their scores on the above variables. The categories were as follows:

None-has not reported any previous victimization

1- one type of previous victimization

2- two types of previous victimization

3- three or more types of previous victimizations

3.7.4 Biometric Familiarity Index

The following 16 variables were used to construct the Biometric Familiarity Index: seen Iris scanning in movies, read about iris scanning, used iris scanning, trust iris scanning, seen facial scanning in movies, read about facial scanning, used facial scanning, trust facial scanning, seen finger scanning in movies, read about finger scanning, used finger scanning, trust finger scanning, seen voice recognition in movies, read about voice recognition, used voice recognition and trust voice recognition. The COUNT command in SPSS was used to create the Biometric Familiarity Index based on the respondents' scores on the questions/variables that make up the index. Individuals who selected between zero and four out of a possible 16 boxes in question one were coded as having a 'low' self-reported level of familiarity with biometrics while those who selected between five and eight boxes in question one were coded as having a 'moderate' self-reported level of familiarity with biometrics. Individuals who had selected more than nine boxes in question one were coded as having a 'high' level of self-reported familiarity with biometrics.

3.7.5 Discrimination Index

The Discrimination Index was created using the COUNT command in SPSS. Questionnaire question # 17 asks respondents to state what types of discrimination they have previously been a victim of and contains eight variables that were used to create this index: age,

gender, ethnicity, race, language, religion, disability, and sexual orientation. Respondents were categorized based on their score on the index:

Never-has not previously been a victim of discrimination

1- one type of previous discrimination

2- two types of previous discrimination

3- three types of previous discrimination

4- four or more types of previous discrimination

3.8 **Analysis**

3.8.1 Descriptive Statistics

Descriptive statistics (frequencies and percentages) were presented to describe the characteristics of the sample in terms of demographic variables as well as the sample's self-reported familiarity with biometric technologies. Frequencies and percentages were also presented for questionnaire question number 2 (for what purposes are individuals willing to provide finger and or facial scans) as well as questionnaire questions five and six which asked respondents whether they support finger/facial scans on passports and why or why not. Frequencies and percentages were also calculated for questionnaire question #19 which asked respondents what type of legislation would need to be implemented when biometric passports are mandated in Canada. Crosstabulations were conducted to numerically present the relationship between victimization and acceptance of finger/facial scan passports; the relationship between perceptions of safety and acceptance of finger/facial scan passports; the relationship between frequency of travel and acceptance of finger/facial scans on passports; the relationship between the level of familiarity with biometrics and acceptance of finger/facial scan passports; as well as the relationship between trust in expert systems and acceptance of finger/facial scans on

passports. Crosstabulations were also used to present the relationship between previous discrimination and the perceived discriminatory nature of biometric passports and the relationship between anxiety towards expert systems and anticipation of discrimination problems associated with biometric passports.

3.8.2 Chi-Square

Chi-square is a non-parametric test of statistical significance used in bivariate tabular analysis. Chi-square measures the strength of association between two variables to determine the likelihood that the association occurred by chance (Babbie, Halley, & Zaino, 2003). This research study used chi-square to test the significance of the relationships between various variables currently under study. The value of chi-square was reported for all crosstabulations presented in the results and analysis sections.

> "In the social sciences researchers agree that the odds must be at least 1 in 20 (i.e., .05) or less (i.e., .02, .01) before we can say that something other than chance must have been operating to produce the observed results. Only at that point, in other words, are researchers prepared to say that a difference they've observed is statistically significant." (Palys, 2003, p.275).

The level of significance used in this report to determine whether a difference is statistically significant will therefore be set at 0.05.

3.8.3 Cramer's V

Cramer's V is a measure of the strength of the association between two categorical variables. Values for Cramer's V range from 0-1, whereas a value closer to 1 indicates an association closer to a perfect association. Babbie, Halley, & Zaino (2003) offer the following guidelines for interpreting the strength of the association:

None	0.00
Weak/Uninteresting Association	.01 to .09

Moderate/Worth Noting	.10 to .29
Strong association/Interesting	.30 to .99
Perfect association	1.00

The value of Cramer's V was reported for all crosstabulations presented in the results and analysis sections of the current study for which a statistically significant relationship existed.

3.8.4 Cronbach's Alpha

Cronbach's Alpha is used to interpret the reliability of an index. Cronbach's Alpha measures the extent to which item responses obtained at the same time correlate with each other. The closer the Cronbach Alpha value is to 1, the higher the reliability is. Conversely, a value closer to 0 signifies a low or non-existing level of reliability. While there is no generally agreed upon cut-off value in the literature a value of 0.70 or higher is generally acceptable however lower thresholds are sometimes used (Nunnally, 1978).

The value of Cronbach's Alpha for The Victimization Index is .565 indicating that the index has a 57% reliability rate. The value of Cronbach's Alpha for the Biometric Familiarity Index .703 indicating 70% reliability. The Cronbach's Alpha value for the Discrimination Index is .552 which indicates a 55% reliability rate.

The methodological decisions and steps outlined above were deemed appropriate by the researcher to answer the questions posed in the current study. The methodological procedure described above produced the results discussed below.

4 RESULTS

4.1 Characteristics of the Sample

As indicated in Table #1 the study sample consisted of 311 students, 35% (n=104) of which were males while 65% (n=194) were females. The average age of respondents was 18 years of age (50% or N=154) while 35% (n=107) reported that they were 19 or 20 years old and 14% (n=43) reported being 21 years of age or older. The majority of students were in their first year of university (67% or N=209), while 16% (n=51) were in their second year of university, 5% (n=16) in their third year of university and finally 7% (n=22) were in their fourth year of university. In terms of area of study 37% (n=108) reported studying in the social science faculty while 13% (n=39) were registered in science faculties, 5% (n=14) in the faculty of management and 46% (n=135) in the arts faculty. Respondents were also asked which Canadian political party they currently support; 15% (n=47) reported support for the New Democratic Party, while 30% (n=92) support the Liberal party, 19% (n=58) support the Conservative party, 1% (n=3) reported support for the Bloc party, and 6% (n=18) reported support for the Green party. Also of note is that 14% (n=44) chose no political party while 11% (n=33) chose the response category of "Don't want to Answer." The religious affiliation for this particular study sample is as follows: 15% (n=44) Protestant Christians, 36% (n=105) Roman Catholics, 1% (n=2) Evangelic Christians, 2% (n=5) Jewish respondents, 5% (n=16) Muslim, 1% (n=3) Hindu, 2% (n=5) Buddhist, 7% (n=20) other and 32% (n=96) reported no religious affiliation. The majority of respondents in this study were white (75% or N=224) while 4% (n=13) reported Arabic/Middle Eastern dissent, 3% (n=10) identified as black, 7% (n=22) as Asian/Pacific Islander, 3% (n=9) reported being bi-racial, and 7% (n=20) in the study sample were a race not listed on the questionnaire.

Table 1 Characteristics of Study Sample (n=311)

Characteristic Variable	N	%
Sex (13missing)		
Male	104	34.9
Female	194	65.1
Age (7 missing)		
18	154	50.7
19-20	107	35.2
21+	43	14.1
Education (13 missing)		
1st yr University	209	67.2
2nd yr University	51	16.4
3rd yr University	16	5.1
4th yr University	22	7.1
Faculty (15 missing)		
Social Science	108	36.5
Sciences	39	13.2
Management	14	4.7
Arts	135	45.6
Party Support (7 missing)		
NDP	47	15.4
Liberal	92	30.2
Conservative	58	19.0
The Bloc	3	1
Green Party	18	5.9
Multiple Parties	9	2.9
None	44	14.4
Don't want to Answer	33	10.8
Religion (15 missing)		
Protestant Christian	44	14.9
Roman Catholic	105	35.5
Evangelic Christian	2	.7
Jewish	5	1.7
Muslim	16	5.4
Hindu	3	1.0
Buddhist	5	1.7
None	96	32.4
Other	20	6.8
Race (13 missing)		
White	224	75.2
Arabic/Middle Eastern	13	4.4
Black	10	3.4
Asian/Pacific Islander	22	7.4
Bi-racial	9	3
Other	20	6.7

A range of crosstabulations were conducted between the various demographic variables and the study's acceptance of biometric passports variables however no significant relationships existed therefore no crosstabs were presented. The demographic variables represent control variables and are unrelated to the hypotheses of the current study.

4.1.1 Self-reported Familiarity of Biometrics

As indicated in Table # 2, 90% of respondents (n=280) have seen iris scanning in movies while 29% (n=90) have read about iris scanning; 3% (n=10) have used iris scanning and 37% (n=114) trust iris scanning to accurately verify their identity. Eighty-eight percent of respondents (n=273) have seen facial scanning technologies in movies whereas 21% (n=65) have read about facial scanning; 5% (n=14) have used facial scanning and 27% (n=83) trust facial scanning. Ninety-one percent of respondents (n=282) have seen finger scanning technologies in movies; 44% (n=137) have read about finger scanning; 32% (n=99) have used finger scanning technologies while 56% (n=173) trust finger scanning technologies to accurately verify their identity. Ninety-two percent of respondents have seen voice recognition technologies in movies; 36% (n=112) have read about voice recognition; 34% (n=106) have used voice recognition technology while 22% (n=67) trust voice recognition technologies to accurately identify them.

Table 2: Questionnaire Question 1

	Seen in Movies	Read About	Used	Trust
Iris Scanning	280 (90%)	90 (29%)	10 (3%)	114 (37%)
Facial Scanning	273 (88%)	65 (21%)	14 (5%)	83 (27%)
Finger Scanning	282 (91%)	137 (44%)	99 (32%)	173 (56%)
Voice Recognition	286 (92%)	112 (36 %)	106 (34%)	67 (22%)

4.2 **Research Question 1**

Research Question 1: In what types of situations are people willing to provide biometric data for identification purposes during a time when science and expert authority is being questioned in the risk society?

Table # 3 illustrates respondents' acceptance for the use of facial and/or finger scanning technologies for various purposes. Thirty-three percent of respondents (n=100) stated a willingness to provide a facial scan to gain access to the workplace while 63% (n=194) were willing to provide a finger scan for this purpose. In order to gain access to a personal computer 17% of respondents (n=52) supported facial scanning while 61% (n=187) supported finger scanning for this purpose. While 51% of respondents (n=157) support facial scanning, 68% (n=211) support the use of finger scanning technologies to cross international borders. Thirty-two percent of respondents (n=99) were willing to provide a facial scan while 50% (n=155) were willing to provide a finger scan to gain access to health services. In order to make purchases 9% of respondents (n=27) were willing to provide a facial scan for identification while 24% (n=75) were willing to provide a finger scan for this purpose. Eighteen percent of respondents (n=55) stated a willingness to provide a facial scan to access an ATM while 46% (n=143) stated a willingness to provide a finger scan to access this service. To obtain a driver's license 41% (n=126) of respondents were willing to provide a facial scan for identification while 55% (n=169) were willing to provide a finger scan to obtain a driver's license. Twenty-seven percent of respondents (n=84) indicated a willingness to provide a facial scan to vote in elections while 53% (n=163) indicated a willingness to provide a finger scan for identification to vote during elections.

Table 3: Facial v Finger Scanning

	A Facial Scan	A Finger Scan
Access Workplace	100 (33%)	**194 (63%)**
Access PC	52 (17%)	**187 (61%)**
Cross international Borders	**157 (51%)**	**211 (68%)**
Access Health Services	99 (32%)	155 (50%)
Make Purchases	27 (9%)	75 (24%)
Access ATM	55 (18%)	143 (46%)
To Obtain Driver's License	126 (41%)	**169 (55%)**
To Vote in Elections	84 (27%)	**163 (53%)**

*Note: **Bolded** figures highlight the acceptance rates that are over 50%.*

4.3 Research Question 2

Research Question 2: Do individual characteristics such as frequency of travel, familiarity with biometrics, anxiety towards expert systems, perceptions of safety or previous victimization contribute to the acceptance or non-acceptance of biometric passports in the risk society?

Hypothesis 1: Previous victimization or negative perceptions of safety will be associated with a greater acceptance of biometric passports.

Null Hypothesis: There will be no association between feelings of vulnerability and the level of acceptance of biometric passports.

As shown in Table # 4, 70% of respondents with no previous victimization (n=60) stated support for biometric passports containing finger scans while 28% (n=24) of respondents with no prior victimization stated acceptance for biometric passports containing facial scans. Seventy percent of respondents who experienced one type of previous victimization (n=59) reported support for biometric passports containing finger scans while 19% of individuals (n=16) who reported one previous type of victimization support passports with facial scans. Of the individuals who reported two previous types of victimization 68% (n=43) stated support for biometric passports containing finger scans while 18% (n=11) stated support for passports containing facial scans. Sixty percent (n=44) of those individuals who reported 3 or more types

of previous victimization stated support for passports containing finger scans while 20% (n=15) stated support for passports containing facial scans. The value of chi-square for the relationship between previous victimization and acceptance of finger scan passports is 2.647 with 3 degrees of freedom which indicates that the relationship is not statistically significant. The chi-square value for the relationship between previous victimization and acceptance of facial scans on passports is 2.868 with 3 degrees of freedom which also indicates that the relationship is not statistically significant. Since the relationship is not statistically significant, the null hypothesis of no difference must be accepted.

Table 4 Victimization & Acceptance of Finger/Facial Scans on Passports

# of Previous Victimizations	Accept Finger Scan Passports	Accept Facial Scan Passports
No Previous Victimization	60 (70%)	24 (28%)
Victimized once	59 (70%)	16 (19%)
Victimized twice	43 (68%)	11 (18%)
Victimized 3 or more times	44 (60%)	15 (20%)
Chi-square	2.647 (df3)	2.868 (df3)

As indicated in Table # 4.1, 67% (n=192) of the individuals who agree that Canada is a safe place to live support the use of finger scans on biometric passports while 22% (n=62) support the use of facial scans on passports. No respondents reported disagreement to the statement that Canada is a safe place to live. Of those individuals who felt that terrorism in Canada is not a risk 59% (n=56) support the use of finger scans for passports while 17% (n=16) support facial scanning technologies for use on biometric passports. Alternatively, 71% (n=27) of those individuals who felt that terrorism is a risk in Canada support the use of finger scans on passports while 27% (n=10) support facial scanning. Sixty-four percent (n=91) of the individuals who felt that the Canadian government effectively addresses national security concerns support the use of finger scanning technologies for biometric passports while 19% (n=25) support the use

of facial scanning for passports. Of those individuals who disagreed with the statement that the Canadian government effectively addresses national security concerns 72% (n=23) support the use of finger scanning for passports while 25 % (n=8) support the use of facial scanning. Sixty-seven percent (n=111) of the respondents who felt that Canada's border was safe support the use of finger scans on passports while 20% (n=33) support the use of facial scanning for biometric passports. Of those respondents who felt that Canada's border was not safe 74% (n=29) support the use of finger scans while 32% (n=12) support the use of facial scanning on biometric passports. Twenty percent (n=33) of those who agreed that the Canadian government protects individual rights support the use of finger scanning technologies on passports while 21% (n=46) support the use of facial scans on passports. Of those respondents who disagree with the statement that the Canadian government protects individual rights 32% (n=12) support finger scans on passports while 15% (n=2) support facial scanning for biometric passports. Sixty-nine percent (n=126) who agreed that the local police do a good job of ensuring neighbourhood safety support the use of finger scanning on biometric passports while 21% (n=38) support the use of facial scanning technology. Of those individuals who felt that the police did not do a good job of ensuring neighbourhood safety, 65% (n=20) support passports containing finger scans while 22% (n=7) support passports containing facial scans. The chi-square values presented in Table # 4.1 returned no statistically significant relationships between the perceptions of safety (vulnerability) and the acceptance of finger/facial scans on passports therefore, the null hypothesis of no difference must be accepted.

Table 4.1 Perceptions of Safety & Acceptance of Finger/Facial Scans on Passports

		Accept Finger Scan Passports	Accept Facial Scan Passports
Canada Safe	Agree	192 (67%)	62 (22%)
	Disagree	0	0
Chi-Square		.437 (df1)	.241 (df1)
Terrorism a Risk	Not a Risk	56 (59%)	16 (17%)
	A Risk	27 (71%)	10 (27%)
Chi-Square		1.695 (df1)	1.746 (df1)
National Security Addressed	Agree	91 (64%)	25 (19%)
	Disagree	23 (72%)	8 (25%)
Chi-Square		.144 (df1)	.685 (df1)
Safe Border	Agree	111 (67%)	33 (20%)
	Disagree	29 (74%)	12 (32%)
Chi-Square		.819 (df1)	2.524 (df1)
Gov't Protects individual rights	Agree	33 (20%)	46 (21%)
	Disagree	12 (32%)	2 (15%)
Chi-Square		2.828 (df1)	.251 (df1)
Local police ensure Safety	Agree	126 (69%)	38 (21%)
	Disagree	20 (65%)	7 (22%)
Chi-Square		.273 (df1)	.020 (df1)

Hypothesis 2: As a result of the efficiency afforded by expert systems of identification individuals who travel more frequently will be more willing to accept biometric passports.

Null Hypothesis: There will be no relationship between the frequency of travel and the level of acceptance of finger and/or facial scan passports.

As depicted in Table # 4.2, 60% (n=56) of respondents who 'rarely' travel (less than once in 5 years) reported support for biometric passports containing finger scans while 16% (n=15) reported support for passports containing facial scans. Of those individuals who reported traveling annually, 73% (n=77) stated support for passports containing finger scans while 22% (n=24) stated support for passports containing facial scans. Sixty-eight percent (n=70) of those who reported traveling outside of Canada two or more times a year support finger scanning technology for passports while 25% (n=25) support the use of facial scanning technology for passports. The chi-square values for the relationship between frequency of travel and acceptance

of finger or facial scans on passports were not statistically significant. Therefore, the null hypothesis must be accepted for this particular relationship within this study sample.

Table 4.2 Frequency of Travel & Acceptance of Finger/Facial Scans on Passports

Travel Outside of Canada	Accept Finger Scan Passports	Accept Facial Scan Passports
Rarely	56 (60%)	15 (16%)
Annually	77 (73%)	24 (22%)
2+ times per yr	70 (68%)	25 (25%)
Chi-Square	4.300 (df2)	2.317 (df2)

Hypothesis 3: Lack of familiarity with expert systems of identification will be associated with a lower level of acceptance of biometric passports.

Null Hypothesis: There will be no relationship between the level of familiarity with biometric technologies and the level of acceptance of finger and/or facial scan passports.

As shown in Table # 4.3, 63% (n=47) of respondents who had a low level of self-reported familiarity with biometrics stated support for passports containing finger scans while 17% (n=13) stated support for the use of facial scans on passports. Of those who had a moderate familiarity with biometric technologies, 62% (n=87) reported support for the use of finger scans on passports while 20% (n=28) reported support for facial scans on passports. Seventy-nine percent (n=72) of those individuals who reported a high familiarity with biometric technologies support the use of finger scans on passports while 28% (n=25) support the use of facial scanning on passports. The chi-square value for the relationship between the level of self-reported familiarity with biometric technologies and the acceptance of finger scans for biometric passports is 8.485 with 2 degrees of freedom which indicates a statistically significant relationship at the 0.05 level of significance. The value of Cramer's V for this relationship is .166 which indicates a moderate relationship that is 17% as strong as a perfect association. The chi-square value for the

relationship between the level of self-reported familiarity with biometric technologies and the acceptance of facial scans for biometric passports was not statistically significant. The null hypothesis of no difference cannot be accepted for finger scans as a relationship exists between the level of familiarity with biometric technologies and acceptance of finger scans on passports. There is no relationship between level of familiarity with biometrics and acceptance of facial scans on passports therefore the null hypothesis of no difference is accepted for this hypothesized relationship.

Table 4.3 Biometric Familiarity & Acceptance of Finger/Facial Scans on Passports

	Accept Finger Scan Passports	**Accept Facial Scan Passports**
Low Familiarity	47 (63%)	13 (17%)
Moderate Familiarity	87 (62%)	28 (20%)
High Familiarity	72 (79%)	25 (28%)
Chi-Square	**8.485 (df2)**	2.968 (df2)
Cramer's V	.166	.098

*Note: **Bolded** figures represent statistically significant relationships. *

Hypothesis 4: Anxiety towards expert systems of identification will be associated with a lower level of acceptance of finger and/or facial scans on passports.

Null Hypothesis: There will be no relationship between the level of anxiety towards expert systems and the level of acceptance of finger and/or facial scans on passports

As shown in Table # 4.4, 75% of respondents (n=84) who trust iris scanning to accurately verify their identity accept the use of finger scans for biometric passports while 27% (n=31) of those who trust iris scanning accept the use of facial scans on biometric passports. Sixty-two percent (n=121) of respondents who stated that they do not trust iris scanning to accurately verify their identity supported the use of finger scans on passports while 18% (n=35) supported facial scanning for biometric passports. Of those individuals who trust facial scanning to accurately verify their identification 77% (n=64) support the use of finger scans on biometric passports

while 35% (n=29) support the use of facial scanning technologies for biometric passports. Of those respondents who do not trust facial scanning to accurately verify their identity 63% (n=141) accept the use of finger scans on passports whereas 17% (n=37) support the implementation of passports with facial scans. Of those individuals who trust finger scanning technologies to accurately verify their identity 77% (n=132) accept the implementation of biometric passports with finger scans while 24% (n=42) accept the use of passports containing facial scans. Of those who reported that they do not trust finger scans to accurately identify them 54% (n=73) accept the use of passports with finger scans while 18% (n=24) support the use of facial scans on passports. Of those respondents who trust voice recognition technologies to accurately verify their identity 74% (n=49) support the implementation of biometric passports containing finger scans while 23% (n=15) support the use of facial scans on biometric passports. Of those who do not trust voice recognition technologies to accurately verify their identity 65% (n=156) support the implementation of biometric passports with finger scans while 21% (n=51) support the use of facial scanning technologies on biometric passports. Of those respondents who were concerned that the databases containing biometric data could be breached 61% (n=117) accept the use of finger scans on passports while 17% (n=32) support the implementation of passports containing facial scans. Of those respondents who are not concerned with a possible breach to biometric databases 70% (n=19) support the implementation of passports with finger scans while 30% (n=8) support facial scan passports. Of those respondents who were concerned that biometric data could be used to track an individuals' activities 60% (n=115) support the implementation of passports containing finger scans while 19% (n=37) support facial scans on passports. Of those individuals who stated that they were not concerned about the possibility of biometric data being used to track people 85% (n=22) support the implementation of passports

containing finger scans while 31% (n=8) support the implementation of passports using facial scans. The chi-square value for the relationship between trusting iris scanning technologies and acceptance of finger scans for biometric passports is 5.121 with one degree of freedom which indicates a statistically significant relationship. The Cramer's V value for this relationship is 0.129 which indicates a moderate association that is 13% as strong as the perfect association. The relationship between trusting facial scanning technologies and acceptance of finger scans on biometric passport is also significant with a chi-square value of 5.270 with one degree of freedom. The value of Cramer's V for this relationship is 0.131 which indicates a moderate association that is 13% as strong as the perfect association. The chi-square for the relationship between concerned about biometric data being used to track people and acceptance of finger scans on biometric passports is also statistically significant with a chi-square of 5.992 with 1 degree of freedom. Cramer's V for this relationship is 0.166 which indicates a moderate association that is 17% as strong as the perfect association. All other relationships in Table # 4.4 were not statistically significant. The null hypothesis of no difference must be rejected for the relationships between trusting iris scanning, trusting facial scanning, concerned about tracking and acceptance of finger scans on passports. The null hypothesis of no difference is therefore accepted for the remaining cells containing a chi-square value that is not displayed in bold font.

Table 4.4 Trust in Expert Systems & Acceptance of Finger/Facial Scans on Passports

		Accept Finger	**Accept Facial**
		Yes	Yes
Trust Iris	Yes	84 (75%)	31 (27%)
	No	121 (62%)	35 (18%)
Chi-Square		**5.121 (df1)**	3.733 (df1)
Cramer's V		.129	.110
Trust Face	Yes	64 (77%)	29 (35%)
	No	141 (63%)	37 (17%)
Chi-Square		**5.270 (df1)**	1.218 (df1)
Cramer's V		.131	.199
Trust Finger	Yes	132 (77%)	42 (24%)
	No	73 (54%)	24 (18%)
Chi-Square		1.824 (df1)	1.976 (df1)
Trust Voice	Yes	49 (74%)	15 (23%)
	No	156 (65%)	51 (21%)
Chi-Square		2.0 (df1)	.075 (df1)
Data Breach	Concerned	117 (61%)	32 (17%)
	Not Concerned	19 (70%)	8 (30%)
Chi-square		.954 (df1)	2.758 (df1)
Tracking	Concerned	115 (60%)	37 (19%)
	Not Concerned	22 (85%)	8 (31%)
Chi-Square		**5.992 (df1)**	1.888 (df1)
Cramer's V		.166	.093

*Note: **Bolded** figure highlights statistically significant relationships. *

4.4 **Research Question 3**

Research Question 3: Do personal vulnerabilities such as previous discrimination and/or anxiety towards expert systems of technology contribute to people's concern about the possible discriminatory consequences of biometric passports in the risk society?

Hypothesis 1: Students who have previously been discriminated against will be more likely to anticipate discrimination problems associated with biometric passports.

Null Hypothesis: There will be no relationship between previous discrimination and anticipation of discrimination problems associated with biometric passports.

As depicted in Table # 5, 31% (n=25) of those who reported no previous discrimination felt that biometric passports could be discriminatory towards people with certain religious beliefs; 61% (n=49) felt that biometric passports could also discriminate against disabled people while 26% (n=21) felt that biometric passports may potentially discriminate against people who simply do not want to provide biometric data for identification purposes. Of those respondents who experienced one type of discrimination 51% (n=38) anticipate that biometric passports could be discriminatory towards people with certain religious beliefs whereas 68% (n=50) anticipated discrimination towards disabled people while 35% (n=26) felt that biometric passports could be discriminatory towards people who did not want to submit their biometric data for identification. Forty-nine percent of respondents (n=41) who experienced two types of discrimination anticipate discrimination towards people with certain religious views while 54% (n=45) anticipate discrimination against disabled people and 36% (n=30) feel that biometric passports could have discriminatory implications towards those people who did not want to provide biometric data for identification purposes. Fifty-six percent of respondents (n=23) who experienced three types of discrimination anticipate discrimination towards people with certain religious views while 66% (n=27) anticipate discrimination against disabled people and 44% (n=18) feel that biometric passports could be discriminatory towards those people who did not want to provide biometric data for identification purposes. Of those respondents who experienced four or more types of discrimination 60% (n=17) anticipate that biometric passports may be discriminatory towards people with certain religious beliefs whereas 79% (n=21) anticipated discrimination towards disabled people while 59% (n=16) felt that biometric passports could discriminate against people who did not want to submit their biometric data for identification. Chi-square values assessing the relationship between previous discrimination and anticipation of discrimination via biometric

passports were not statistically significant. Therefore the null hypothesis of no difference must be accepted.

Table 5 Previous Discrimination & Anticipated Discrimination

# of Types of discrimination	Feel Biometric Passports Discriminate v. religious	Feel Biometric Passports Discriminate v. disabled	Feel Biometric Passports Discriminate v. others
Never	25 (31%)	49 (61%)	21 (26%)
1 type	38 (51%)	50 (68%)	26 (35%)
2	41 (49%)	45 (54%)	30 (36%)
3	23 (56%)	27 (66%)	18 (44%)
4+	17 (60%)	21 (79%)	16 (59%)
Chi-Square	1.32 (df4)	6.695 (df4)	1.102 (df4)

Hypothesis 2: Anxiety towards expert systems of technology will be associated with a greater anticipation of discrimination problems associated with biometric passports.

Null Hypothesis 2: There will be no relationship between anxiety in expert systems of technology and the anticipation of discrimination problems associated with biometric passports.

As indicated in Table # 5.1, 57% of respondents (n=108) who are concerned that the databases containing biometric data could be breached anticipate that biometric passports could be discriminatory towards people with certain religious beliefs; 70% (n=134) felt that biometric passports may discriminate against disabled people while 44% (n=84) felt that biometric passports may be discriminatory towards those people who simply do not want to provide biometric data for the purpose of identification. Of those respondents who were not concerned about the possibility of a data breach 22% (n=6) anticipate that biometric passports would be discriminatory towards people with certain religious beliefs whereas 48% (n=13) anticipated discrimination towards disabled people while 22% (n=6) felt that biometric passports could be discriminatory towards other people who did not want to submit their biometric data for identification. Of those respondents who were concerned about biometric data being used to

track people 50% (n=97) anticipate that biometric passports may be discriminatory towards religious people whereas 64% (n=124) anticipated discrimination towards disabled people while 43% (n=82) felt that biometric passports could be discriminatory towards people who did not want to submit their biometric data for identification. Nineteen percent (n=5) of respondents who were not concerned about biometric data being used to track individuals felt that biometric passports may discriminate against religious people while 46% (n=12) anticipate possible discrimination against disabled people and 12% (n=3) felt that biometric passports may discriminate against those people who do not wish to provide biometric data for the purpose of identification. The relationship between concerned about breaches to a biometric database and feeling that biometric passports could discriminate against disabled people is statistically significant with a chi-square value of 5.218 with 1 degree of freedom. Cramer's V for this relationship is 0.155 which indicates a moderate association that is 16% as strong as the perfect association. The relationship between concerned about breaches to a biometric database and feeling that biometric passports would discriminate against other people who did not want to provide biometric data for identification is also statistically significant with a chi-square value of 4.619 with 1 degree of freedom. Cramer's V for this relationship is 0.146 which indicates a moderate association that is 15% as strong as the perfect association. The relationship between concerned about biometric data being used to track people and the anticipation that biometric passports may discriminate against people with religious beliefs that prohibit them from providing biometric data for identification is significant with a chi-square value of 8.866 with one degree of freedom. Cramer's V for this relationship is 0.201 which indicates a moderate association 20% as strong as the perfect association. The chi-square value for the relationship between concerned with tracking and anticipation of discrimination against people who simply

do not want to provide biometric data for identification purposes is 9.241 with one degree of freedom indicating a statistically significant relationship. Cramer's V for this relationship is 0.205 which is a moderate association that is 21% as strong as the perfect association. The null hypothesis is accepted for the relationships between concerned with data breach and anticipation of discrimination towards religious people as well as the relationship between concerned with tracking and potential discrimination towards disabled people. The null hypothesis is rejected for all other relationships displayed in the table below indicated by a bolded chi-square figure.

Table 5.1 Data Breach/Tracking & Anticipated Discrimination

Concerned with Data Breach	Discrimination v religious People	Discrimination v Disabled	Discrimination v others
Concerned	108 (57%)	134 (70%)	84 (44%)
Not Concerned	6 (22%)	13 (48%)	6 (22%)
Chi Square	1.117 (df1)	**5.218 (df1)**	**4.619 (df1)**
Cramer's V	.226	.155	.146
Concerned with Tracking			
Concerned	97 (50%)	124 (64%)	82 (43%)
Not Concerned	5 (19%)	12 (46%)	3 (12%)
Chi Square	**8.866 (df1)**	3.188 (df1)	**9.241 (df1)**
Cramer's V	.201	.121	.205

*Note: **Bolded** figures represent statistically significant relationships. *

As indicated in Table # 5.2 (below), 33% (n=27) of people who trust facial scanning to accurately identify them feel that biometric passports may be discriminatory towards people with religious beliefs who will not submit biometric data for the purpose of identification; while 51% (n=42) who trust facial scanning felt that biometric passports discriminated against disabled people who are unable to submit biometric data; of those who trust facial scanning 26% (n=21) felt that biometric passports may be discriminatory against people who do not want to provide biometric data for identification purposes. Conversely, 52% (n=116) of respondents who do not trust facial scanning technologies felt that biometric passports could potentially be

discriminatory against people with religious beliefs; 67% (n=149) felt biometric passports could discriminatory towards people with disabilities while 40% (n=90) felt that biometric passports may be discriminatory against people who simply do not want to provide biometric data for the purpose of identification. Table # 5.2 also indicates that 48% (n=81) of the respondents who trust finger scanning to accurately verify their identity felt that biometric passports may be discriminatory towards people with certain religious beliefs while 63% (n=107) felt that biometric passports discriminated against disabled people and 31% (n=53) felt that biometric passports were potentially discriminatory towards people who did not want to submit biometric data for identification purposes. Forty-six percent of respondents (n=62) who do not trust finger scanning technologies felt that biometric passports may be discriminatory towards people with religious beliefs while 62% (n=84) of respondents felt that biometric passports could discriminate against disabled people and 43% (n=58) felt that biometric passports could be discriminatory towards those people who simply do not want to provide biometric data for identification. The relationship between trusting facial scanning technologies and anticipating discrimination problems against people with certain religious beliefs who do not want to provide biometric data for identification purposes is significant with a chi-square value of 8.576 with one degree of freedom. Cramer's V for this relationship is 0.167 which is a moderate association that is 17% as strong as the perfect association. Chi-square for the relationship between trusting facial scanning and anticipating discrimination problems associated with biometric passports and disabled people is 5.989 with one degree of freedom which is statistically significant. Cramer's V for this relationship is 0.140 which indicates a moderate association that is 14% as strong as the perfect association. A statistically significant relationship also exists between trusting facial scanning technologies and anticipating discrimination via biometric passports towards those

people who do not want to submit biometric data for identification. Chi-square for this relationship is 5.512 with one degree of freedom. Cramer's V for this relationship is 0.134, a moderate relationship that is 13% as strong as the perfect association. The relationship between trusting finger scanning technologies and anticipating discrimination towards people who do not want to provide biometric data for identification is statistically significant with a chi-square value of 4.301 and one degree of freedom. Cramer's V for this relationship is 0.119 which indicates a moderate association 12% as strong as the perfect association. The hypothesis of no difference is accepted for the relationship between trust in finger scanning and discrimination against religious people as well as for the relationship between trust in finger scanning and possible discrimination towards disabled people. The null hypothesis of no difference is rejected for the remaining relationships displayed in Table #5.2 indicated in bold font.

Table 5.2 Trust Finger/Facial Scanning & Anticipation of Discrimination

Trust Facial Scanning	Discrimination v Religious People	Discrimination v Disabled	Discrimination v Others
Yes	27 (33%)	42 (51%)	21 (26%)
No	116 (52%)	149 (67%)	90 (40%)
Chi-Square	**8.576 (df1)**	**5.989 (df1)**	**5.512 (df1)**
Cramer's V	.167	.140	.134
Trust Finger Scanning			
Yes	81 (48%)	107 (63%)	53 (31%)
No	62 (46%)	84 (62%)	58 (43%)
Chi-Square	.129 (df1)	.045 (df1)	**4.301 (df1)**
Cramer's V	.021	.012	.119

*Note: **Bolded** figures represent statistically significant relationships. *

4.5 **Research Question 4**

Research Question 4: Has the normalization of extraordinary technologies garnered greater support for facial scanning technologies or is finger scanning the preferred method of biometric identification?

Table #6 is a numeric representation of the responses to questionnaire question two which asked respondents to state whether or not they would be willing to provide finger scans and/or facial scans to gain access to certain places and services. Sixty-three percent of respondents (n=194) stated that they would be willing to provide a finger scan to gain access to their place of work while 33% (n=100) stated that they would be willing to provide a facial scan to access their workplace. Sixty-one percent of respondents (n=187) stated that they would be willing to provide a finger scan to access their personal computer while 17% (n=52) stated that they would be willing to provide a facial scan to access their personal computer. Sixty-eight percent of respondents (n=211) reported that they would be willing to provide a finger scan to cross international borders while 51% (n=157) reported a willingness to provide facial scans to cross international borders. Fifty percent of respondents (n=155) stated that they would support the use of finger scans to gain access to health services while 32% (n=99) reported a willingness to provide a facial scan to gain access to health services. Twenty-four percent of respondents (n=75) stated that they would be willing to provide a finger scan to make purchases while 9% (n=27) stated that they would be willing to provide a facial scan for this purpose. Forty-six percent of respondents (n=143) stated that they would accept the use of finger scans for identification purposes to access an ATM (automated teller machine) while 18% (n=55) would be willing to provide a facial scan to access an ATM. Fifty-five percent of respondents (n=169) reported a willingness to provide finger scans to obtain a driver's license while 41% (n=126) were willing to provide a facial scan to obtain a license. Fifty-three percent of respondents (n=163) stated that they would be willing to provide a finger scan in order to vote in elections while 27% (n=84) were willing to provide a facial scan to vote. Table # 4 is not a crosstabulation

between two variables therefore no tests of significance can be performed. However, the data illustrates a clear preference for finger scans to gain access to the various services listed below.

Table 6 Questionnaire Question 2

	A Finger Scan	A Facial Scan
Access Workplace	**194 (63%)**	100 (33%)
Access PC	**187 (61%)**	52 (17%)
Cross international Borders	**211 (68%)**	157 (51%)
Access Health Services	**155 (50%)**	99 (32%)
Make Purchases	**75 (24%)**	27 (9%)
Access ATM	**143 (46%)**	55 (18%)
To Obtain Driver's License	**169 (55%)**	126 (41%)
To Vote in Elections	**163 (53%)**	84 (27%)

*Note: **bolded** figures indicate biometric preference for that particular service.

As indicated in Table # 6.1(below), 67% of respondents (n=206) support the implementation of passports containing finger scans. Of those who support finger scan passports 50% (n=103) indicated that these passports would be convenient while 85% (n=175) felt that they would be secure; 71% (n=147) felt that they would ensure personal safety whereas 81% (n=168) supported finger scan passports for national security reasons. Twenty-one percent of respondents (n=66) support the implementation of passports containing facial scans. Of those who support facial scans on passports 39% (n=26) of respondents citing its convenience; 83% (n=55) its' secure technology; 79% (n=52) personal safety; and 77% (n=51) stated national security as reasons for supporting facial scan passports.

Thirty-three percent of respondents (n=101) did not support the use of finger scans on passports. Fifty-six percent of respondents (n=57) cited privacy concerns; 51% (n=52) were fearful of identity theft; 47% (n=47) were unsure of the technology; 59% (n=60) cited high cost while 67% (n=68) were fearful about abuse of information and six percent (n=6) cited religious views as reasons for not supporting finger scan passports. Seventy-nine percent of respondents (n=242) did not support the implementation of passports containing facial scans. Of those who

did not support facial scan passports 50% (n=120) cited privacy concerns; 43% (n=104) were fearful of identity theft; 66% (n=160) were unsure of technology; 71% (n=172) cited high costs while 57% (n=138) were fearful about abuse of information and 10% (n=23) cited religious views as reasons for not supporting facial scan passports. Table # 4.1 is not a crosstabulation between variables therefore no tests of significance can be performed. However, the data indicates that finger scans are preferred over facial scans on passports.

Table 6.1 Reasons for Acceptance of Finger/Facial Scans on Passports

	Support Finger Scan Passports	**Support Facial Scan Passports**
Yes	**206 (67%)**	**66 (21%)**
Convenient	103 (50%)	26 (39%)
Secure	175 (85%)	55 (83%)
Personal Safety	147 (71%)	52 (79%)
National Security	168 (81%)	51 (77%)
No	**101 (33%)**	**242 (79%)**
Privacy Concerns	57 (56%)	120 (50%)
Identity Theft	52 (51%)	104 (43%)
Unsure of Technology	47 (47%)	160 (66%)
High Cost	60 (59%)	172 (71%)
Possible Abuse of Information	68 (67%)	138 (57%)
Religious Views	6 (6%)	23 (10%)

4.6 **Respondents' Perceptions of Policy Implications**

While not a specific research question of the current study, questionnaire question #19 asked respondents to indicate what type of legislation they felt would need to be implemented when biometric passports are issued in 2011. Responses to this question are provided below.

As depicted in Table # 6, 90% of respondents (n=277) felt a need to implement legislation to protect informational privacy to regulate who can access stored biometric data when biometric passports are implemented in Canada. Seventy-seven percent of respondents (n=238) felt that legislation giving people the right to know how biometric data is stored should

be implemented when biometric passports are mandated in Canada. Seventy-nine percent of respondents (n=244) wanted legislation that states the purpose of biometric data collection to prevent improper use of data to be implemented. Forty-three percent of respondents (n=133) would like to see legislation to protect the rights of religious people implemented. Fifty-four percent of respondents (n=166) felt that legislation protecting the rights of disabled people would be necessary when biometric passports are mandated in Canada. Two percent of respondents (n=7) felt that no legislation would be necessary when biometric passports are implemented in Canada while 5% (n=15) felt that some other type of legislation would also need to be implemented along with biometric passports. Table # 6 is not a crosstabulation between two variables therefore no tests of significance can be performed to interpret the relationship; however, the data indicates that respondents are very concerned with protecting the privacy of their biometric data.

Table 6 Type of Legislation Needed

Type of Legislation Survey Respondents deemed important	N	%
Legislation protecting informational privacy to regulate who can access biometric data	277	90
Legislation giving people the right to know how their biometric data is stored	238	77
Legislation stating the purpose of collection	244	79
Legislation Protecting religious People	133	43
Legislation Protecting disabled people	166	54
No legislation needed	7	2
Other	15	5

Protecting user privacy is a major concern that needs to be addressed through technological advancements as well as policy implementation. Technology is capable of performing remarkable tasks but all the elements and potential implications of these feats must be considered to alleviate as many negative consequences as possible. Effective policies need to be implemented to ensure the safe storage of data, to outline who can access the data and what specifically the data can be used for.

5 DISCUSSION

The table outline provided directly below is a summary of the major relationships noted above, provided as a guide to the discussion that follows.

Table 7 Summary of Main Findings

Research Question 4: finger scans v facial scans

People were more accepting of finger scans to:

- •Access a Workplace
- •Cross international Borders
- •Make Purchases
- •To Obtain Driver's License
- •On biometric Passports
- •Access a PC
- •Access Health Services
- •Access an ATM
- •To Vote in Elections

Research Question 1: When are people willing to provide biometric data for identification?

- To cross the border #1 response for both finger and facial scans
- To obtain a driver's license #2 response for facial scans (41% acceptance)
- To access the workplace #2 response for finger scans (63% acceptance)

Research Question 2: What personal traits contribute to the acceptance of biometric passports?

- More familiarity with biometrics is associated with a greater acceptance of finger scan passports
- Trust in iris or facial scans is associated with a higher acceptance of finger scan passports
- Respondents concerned about data being used to track people were less accepting of finger scan passports than respondents who were not concerned about tracking

Research Question 3: What vulnerabilities are associated with discrimination concerns?

- Individuals concerned with a data breach are more likely to anticipate:
  - Discrimination towards disabled people
  - Discrimination towards others who do not want to submit biometric data
- Individuals concerned with tracking are more likely to anticipate:
  - Discrimination towards people with certain religious beliefs
  - Discrimination towards others who do not want to submit biometric data
- Individuals who do not trust facial scanning are more likely to anticipate:
  - Discrimination towards people with certain religious beliefs
  - Discrimination towards disabled people
  - Discrimination towards others who do not want to submit biometric data
- Individuals who do not trust finger scanning are more likely to anticipate:
  - Discrimination towards others who do not want to submit biometric data

The focus of the current study was to expand the current knowledge regarding the paradox highlighted by Van Loon (2000) and other risk society theorists concerning the increasing role of science and technology for managing risks during a time when the epistemology of science is facing severe criticism for failing to manage these risks. Empirically, this study examined how perceived risks and the normalization of extraordinary technologies have affected people's perceptions regarding the need for heighten measures of security, namely biometric passports. A sample of English speaking students in first year courses at the University of Ottawa were selected to participate in this study by responding to a group-administered questionnaire regarding when they would be willing to accept the use of biometric technologies for identification purposes.

Thematically, the research questions of the current study explored the nature of the hypothesized ambivalent relationship people have towards science and technology by identifying the purposes for which people were willing to accept the use of biometric identification, and by determining the preferred biometric identifier and the reasons for this preference. While the integration of extraordinary technologies into the everyday lives of individuals has brought forth a greater acceptance of the technologies, they have also enabled greater risk detection, which highlights the omnipresence of risk and heightens fear of crime. Therefore the current study examined whether personal characteristics such as previous victimization, negative perceptions of safety and/or anxiety towards expert systems were associated with the acceptance or non-acceptance of biometric passports in the risk society. The current study also examined various personal vulnerabilities including previous discrimination and anxiety towards science and experts to explore whether these vulnerabilities were associated with people's perceptions regarding the potential discriminatory consequences of biometric passports. Biometrics have

permeated various facets of society and as such a discussion regarding the normalization of technology is provided below followed by a discussion about scientific expertise.

Risk assessment, surveillance and identification technologies have become the main pillars of safety initiatives and security policies alike (Ceyhan, 2006). The methods of identification that were previously used to identify immigrants or marginalized populations have expanded and are now used to identify entire populations. During a time when definitions of risk are proliferating and uncertain risks are increasing, technological solutions are sought to assess these risks and to protect against crime and terrorism (Ceyhan, 2006). Finger scans and facial scans are the biometric identifiers most commonly used or proposed for use on national ID cards and electronic passports. The International Civil Aviation Organization (ICAO) recommended facial scans as the most interoperable identifier even though finger scanning technology is considered to have a higher accuracy rate than facial scanning. Both the ICAO and the European Commission recommend the use of facial scanning as the primary biometric indicator on identification documents (Liberatore, 2007). In spite of this, the integration of extraordinary technologies into the daily lives of individuals has brought about an increasing acceptance of finger scanning technologies and to a lesser extent facial scanning technologies. Related findings are discussed below.

Finger print identification has been used since the 18th century and has become cheaper and easier to implement and therefore widely used throughout society (Privacy and Technologies of identity, 2006). While frequently associated with criminality, finger scanning is gaining popularity as an acceptable security feature to protect laptops, cell phones, and to gain access to restricted areas. This integration of biometric technologies into the daily lives of individuals makes users more comfortable with the technology and thus more accepting of the technology

for identification purposes (Liberatore, 2007). As indicated in Table #3 over 50% of respondents stated a willingness to provide a finger scan to: cross international borders (68%), access the workplace (63%), access a personal computer (61%), obtain a driver's license (55%) and to vote in elections (53%); while 50% supported the use of finger scans to access health services, 46% were willing to provide a finger scan to access an ATM and 24% stated a willingness to provide a finger scan to make purchases. These acceptance rates are much higher than the acceptance rates for facial scanning technologies as outlined below.

Facial scanning is becoming increasingly popular and expanding into commercial and domestic spheres however, it does not currently possess the long established history of use similar to that of finger print identification. Even though the face is an individual's most visible feature and facial scanning is frequently portrayed in popular sci-fi movies, facial scanning did not receive the same level of support in the current study as finger scanning. As indicated in Table # 3, 51% of respondents stated a willingness to provide a facial scan to cross international borders while less than 50% supported the various other uses of facial scanning technologies such as: obtaining a driver's license (41%), accessing the workplace (33%), accessing health services (32%), voting in elections (27%), accessing an ATM (18%), securing a personal computer (17%), or making purchases (9%). These particular findings are not in line with the literature pertaining to the social acceptance of biometric technologies which highlights a lower level of acceptance for finger scan technologies due to their association with criminal investigations (Liberatore, 2007; Nanavati, Thieme & Nanavati, 2002; Reid, 2004; & Woodward, 2008). Finger scanning technologies have a higher accuracy rate than facial scanning technologies (Liberatore, 2007), have an established history of use (Nanavati, Thieme & Nanavati, 2002), and are identified as the preferred biometric identifier among participants in the

current study. The acceptance rates noted above provide a comparison between finger and facial scanning technologies for various purposes. Both finger and facial scanning technologies received the highest acceptance rate for use when crossing an international border. Therefore, a discussion regarding the use of biometric technologies specifically at the border follows.

Examining the biometric technologies more specifically in terms of their acceptance for use on biometric passports elicits the same pattern of acceptance highlighted above. As indicated in Table # 6.1, 67% of respondents (n=206) support the use of finger scans on passports while only 21% (n=66) support the use of facial scanning for biometric passports. Reasons associated with the acceptance of biometric passports containing finger scans included: secure technology (85%), national security (81%), personal safety (71%) and convenience (50%). Two of the main advantages of finger scanning for users of biometric identification are fingerprints' uniqueness and immutability (Wayman et al., 2005). The accuracy rate of fingerprint identification is extremely high due to the amount of discriminatory information contained in fingerprints. Even identical twins will have different finger print characteristics (Wayman et al., 2005). The immutability of fingerprints refers to its' stability over a lifetime. While fingerprints are susceptible to ware over time, the specific features and minute characteristics remain constant (Wayman et al., 2005). The two basic features of fingerprints noted above ensure a high accuracy rate and therefore a high acceptance rate amongst users of the technology.

The reasons associated with the lack of acceptance of facial scans on biometric passports in the current study included: high cost (71%), unsure of technology (66%), possible abuse of information (57%), privacy concerns (50%), possible identity theft (43%) and religious views (10%). The literature regarding user acceptance of facial scanning also highlights the hesitation towards the use of this type of technology and concerns regarding the possible abuse of

information (Nanavati, Thieme & Nanavati, 2002). Many users of biometric identification are aware of the non-cooperative nature of facial scanning technologies and that these technologies have the ability to capture, store, and process a digital imagine without the subject's knowledge (Nanavati, Thieme & Nanavati, 2002). The collection of facial scans, covertly or otherwise, would enable the creation of a database that contained an image of every citizen, which could lead to the possible abuse of information if it was used to track people. Many of the concerns of the current study are reiterated in the existing literature; however, some of the specific results are not.

The particular findings of the current study regarding user acceptance of finger and facial scanning do not support the recommendations of the ICAO or the ideal biometric scores cited in Reid, 2004. The ICAO recommended the use of facial scans as the primary identifier on biometric passports and the use of finger scans as a secondary identifier if needed (Liberatore, 2007). According to the ideal biometric score, fingerprint technology rated closest to the ideal biometric for its deployability, robustness, maturity, and general suitability while facial scanning technologies ranked the highest in terms of user acceptance (Reid, 2004). The varied findings reported in a range of studies supports the hypothesis that people have an ambivalent relationship towards science and technology, as similar levels of acceptance of biometrics are not standard throughout the studies. Part of this ambivalence may stem from the nature of the various study samples. Studies taking place in countries where biometric passports are already in use, such as Germany or Australia for example, are conducted on samples of the population who have already been exposed to the use of biometric passports whose views of the technology may differ from the views of individuals who have not been exposed to the use of biometric passports. Furthermore, the current study surveyed a student population whose perceptions of the use and

need for biometric passports may greatly differ from the views of a business person, for example, who frequently travels and is therefore a member of an expedited traveler program that currently uses biometric technologies. The sample used in the current study is merely a subset of the population of future users of biometric passports and therefore a future study using other subsets of future users is needed to confirm or disconfirm the hypotheses in this study.

The variance between the rates of acceptance for finger and facial scanning technologies for identification purposes is one element of the ambivalent relationship people have towards science and experts. Many respondents stated that they have privacy, security, and technological concerns about biometric technologies; which is interesting to note because 67% of the respondents accepted the use of finger scans on passports while only 21% accepted facial scanning on passports. The need to effectively identify and manage risks is evident within the risk society; however there is a lack of consensus regarding the best way to manage these risks. Within the context of the current study finger scans were identified as the preferred biometric identifier despite their association with criminal law enforcement investigations. Finger scanning technologies were effectively integrated into the everyday lives of individuals over a long period of time which enabled users to become familiar and accepting of the technology. While initially used to identify prisoners and asylum seekers, the easy-to-use finger scan devices are now employed in a wide range of environments to monitor school attendance, to control access to restricted areas, to enhance security on cell phones and laptops, and to verify one's identity for various other purposes (Nanavati, Thieme & Nanavati, 2002). This gradual integration of finger scanning technology into the everyday lives of individuals is therefore a condition of possibility for the higher acceptance of finger scans for identification purposes. Aside from its established history of use and gradual integration into routine daily activities, the higher acceptance rate of

finger scans over facial scans is interesting to note because people are usually accepting of various types of technologies or are against technology altogether. This acceptance of some biometric technologies but not others is part of the ambivalent relationship people have towards science as discussed below as the second major theme of the current study.

Expert systems of technology are increasingly being sought to manage risks during a time when science and expert authority are being questioned and criticized for not effectively managing these risks (Eckberg, 2007; & Giddens, 1996). At times, expert systems of technology are deemed highly innovative and extremely efficient. However, these technologies also increase the knowledge and awareness of risk to a level where even the technologies that detect the risks cannot manage them.

Continued research into the areas of crime prevention and management is needed in order to stay up to date with the increasingly global risks that plague today's networked society; however the continued research into a specific area maintains the fear associated with that particular fear or problem (Lee, 2001). This feedback loop reinforces fear of crime as people need to be aware of crime to fear it. When the technologies that are used to manage risks highlight the omnipresence of risk, people become more aware of these risks and seek out expert systems to manage them. Therefore it was hypothesized that an individual's perception of safety would be related to their acceptance of biometric passports in terms of a higher level of acceptance associated with perceptions that Canada and/or its citizens are unsafe. Seventy-one percent of individuals who felt terrorism was a risk in Canada accepted the use of finger scans on passports compared to a 59% acceptance rate among individuals who felt that terrorism was not a risk in Canada. Additionally, 27% of individuals who felt that terrorism was a risk in Canada support the use of facial scans on passports compared to a 17% acceptance rate among

individuals who felt that terrorism was not a risk in Canada. Of those individuals who felt that Canada's border was safe, 67% support the use of finger scans on biometric passports compared to an acceptance rate of 74% amongst individuals who felt that Canada's border was not safe. Moreover, 20% of individuals who felt that Canada's border was safe accepted the use of facial scans on biometric passports compared to an acceptance rate of 32% amongst individuals who felt that Canada's border was not safe.

While not a statistically significant relationship, within the current study a greater acceptance of biometric passports was associated with perceptions that Canada's border is not safe and perceptions that terrorism is a risk in Canada. This particular finding is interesting to note as originally it was hypothesized that previous victimization and feelings of personal vulnerability would be associated with a greater acceptance of biometric passports however, evidence suggests that individuals who have perceptions of vulnerability as it relates to national security (threats at the border and/or a risk of terrorism) are associated with a greater acceptance of biometric passports. This particular finding supports Garland's (2003) assertion that people tend to overestimate the frequency of low-probability, high consequence events such as plane crashes and national security risks while underestimating the frequency of high-probability, low consequence events such as accidents around the home or on the road. These shared feelings of vulnerability and insecurity give rise to an increasing urgency to control, segregate, fortify and exclude (Garland, 2001). Security is designed to manage space and separate people which fuels the fixation regarding the need to monitor risky individuals, to isolate dangerous populations, and to erect situational controls on previously open environments (Garland, 2001). The technological methods of identification increasingly sought for use at border crossings may be capable of identifying more risks than previous methods of identification however, the science

behind these technologies still faces criticism when the system fails to properly manage a risk or when an individual's rights are at risk.

Technologies within a network society have a highly contradictory component whereby the technologies that are designed to mitigate fears may simultaneously reinforce those fears (Liberatore, 2007). An individual who is familiar with the technology may feel safe using or being subjected to surveillance and identification technologies while someone who is not familiar with the technology may become fearful and wonder why they are being screened or asked to provide finger prints. This uncertainty also evokes suspicion regarding how the collected data can be used and the potential for misuse of information. While technological solutions may provide a heightened sense of control and security these solutions may simultaneously increase people's fears that something bad could happen (Liberatore, 2007). Therefore, it was hypothesized that those individuals who had a higher level of familiarity with expert systems of identification would have a higher level of acceptance for biometric passports. As shown in Table # 4.3, a statistically significant relationship exists between the level of familiarity of biometric technologies and the acceptance of finger scans on passports. Sixty-three percent of individuals with a low familiarity of biometric technologies accepted the use of finger scans on passports while 79% of respondents with a high familiarity with biometric technologies supported the use of finger scans on biometric passports. Furthermore, only 17% of individuals with a low familiarity of biometric technologies accepted the use of facial scans on passports while 28% of respondents with a high familiarity with biometric technologies supported the use of facial scans on passports. The integration of technologies into the daily lives of individuals familiarizes people with the technology, which makes them more comfortable and accepting of

the technology. This gradual acceptance is a building block to forming a relationship of trust between the users and the creators of the technology a theme discussed below.

Related to the above discussion, and a main theme throughout the current study, it was hypothesized that anxiety towards expert systems would result in a lower level of acceptance of biometric passports and that trust in expert systems of identification would therefore garner greater support for biometric passports. Some respondents may trust biometric technologies because they possess a prior knowledge of them or have become familiar with them, while others may trust the proven performance of the technology or the standards and credentials of the experts who back these technologies. As depicted in Table #4.4, 75% of individuals who trust iris scanning to correctly identify them accept the use of finger scans on passports compared to a 62% acceptance rate for finger scans on passports among individuals who do not trust iris scanning. Additionally, 27% of individuals who trust iris scanning support the use of facial scans on biometric passports compared to an 18% acceptance rate of facial scans on passports amongst respondents who do not trust iris scanning. Similar patterns exist for the relationships between trust in facial scanning, finger scanning, voice recognition systems and the acceptance of finger and facial scanning on passports (see Table# 4.4). Furthermore, 70% of individuals who were not concerned about breaches to biometric databases accepted the use of finger scans on passports compared to an acceptance rate of 61% amongst individuals who feared breaches to biometric databases. Additionally, 85% of individuals who were not concerned that biometric information would be used to track them supported the use of finger scans on passports compared to a 60% acceptance amongst individuals who feared tracking. Similar patterns exist between fearing data breaches and tracking and the acceptance of facial scanning on biometric passports (see Table # 4.4).

The trust that individuals had as a result of being part of a shared identity routed in kinship in previous eras shifted after the collapse of the welfare state to a trust relationship characterized by faceless trust in symbolic tokens (such as money) and unfamiliar social systems (such as expert systems of technology) (Giddens, 1990). Technological advances throughout the world have transformed the nature of risk, risk assessment and risk management. Even though science and expert opinions are no longer considered the only legitimate truths, expert systems of technology are sought to manage the risks of the increasingly global world. Individuals who are unfamiliar with biometric technologies are urged to trust the legitimacy of the professional standards of expert systems, the reputation of the experts and the performance of the technologies to manage the risks that we can no longer manage ourselves (Giddens, 1990).

Related to the above discussion regarding the ambivalent relationship that appears to exist in terms of seeking out expert systems of identification during a time when science and expert authority is being questioned is research question number three, which relates to discrimination as a result of the implementation of biometric passports. It was hypothesized that anxiety towards expert systems of identification would be associated with a greater anticipation of discrimination associated with biometric passports. As indicated in Table # 5.1, 57% of individuals who were concerned with breaches to biometric databases and only 22% of individuals who were not concerned with data breaches anticipate discrimination towards religious people due to the implementation of biometric passports. Moreover, 70% of individuals who were concerned with breaches to biometric databases and 48% of respondents who were not concerned about breaches anticipated discrimination towards disabled people as a result of the implementation of biometric passports. Similar results exist for the relationship between concerned about tracking via biometric data and the anticipation of discrimination (see Table #

5.1). Furthermore, Table # 5.2 indicates that 33% of people who trust facial scanning and 48% of individuals who trust finger scanning anticipate discrimination towards people with certain religious views when biometric passports are implemented in Canada. Moreover, Table # 5.2 indicates that 51% of people who trust facial scanning and 63% of people who trust finger scanning anticipate discriminatory consequences towards disabled people as a result of the mandated use of biometric passports in Canada. The percentage of individuals who trust expert systems to accurately identify them despite their concerns about the technology's discriminatory potential is further evidence to support the notion that people have an ambivalent relationship towards science and technology. Overall, 63% of respondents (n=192) feel that biometric passports could discriminate against people with disabilities; 47% of respondents (n=144) feel that biometric passports may discriminate against people with certain religious views; and 36% of respondents (n=111) feel that biometric passports may also discriminate against other people who simply do not want to submit biometric data for identification purposes.

It is possible that people accept the use of biometric technologies despite their discriminatory potential because people do not want to face the increasingly global risks alone. The omnipresence of risk has made people more aware of the potential risks that plague society and potentially more accepting of the potential consequences of the use of biometric technologies because they feel there is no viable alternative. While biometric technologies may discriminate against certain sectors of the population, the safety and security of the nation state takes precedence. Conversely, some people may not be aware of the potential discriminatory consequences that can stem from biometric passports. An individual who is not adversely affected by biometric technology may not be aware of its potential implications and may therefore, be accepting of the technology.

Discrimination is an interesting facet of the ambivalent relationship people have towards science and experts. Discrimination divides the population and essentially signifies an acceptance of exclusion in the name of security. Members of the public are often subjected to contradictory opinions or not given enough objective information to formulate an informed opinion. The resulting relationship towards expert systems of technology designed to make people feel safer is that of ambivalence.

Attempting to break down this ambivalent relationship to discern whether people are ambivalent towards experts or science itself proves difficult, as it can be argued that the two are co-dependent. One facet of this relationship therefore, could not exist without the other. According to Elia Zureik (2004) surveillance technologies are examined in routine daily activities and as such are construed as trust-enhancing tools. The more effective these tools are at accurately identifying people the more trustworthy these technologies are perceived to be. Therefore, writes Zureik (2004, p.118), "if trust in institutions depends on the type of technology in use, trust in technology is also a function of level of trust in institutions that use the technology to begin with." Citizens' willingness to drink tap water, take medication, and fly 30,000 feet above the ground is dependent upon a certain level of established trust and confidence in the systems that deliver these services to meet prescribed safety standards (Garland, 2003). Authorities attempt to establish and maintain trust towards the institutions that provide these services by creating a framework of legislation and meticulous inspection to ensure the highest standards are met thus allowing individuals to perform routine activities without hesitation (Garland, 2003). Unfortunately, strict adherence to safety standards is not effective when experts provide conflicting information nor can it prevent unintended consequences. As citizens learn more about science and technology they become increasingly aware that science is

fallible and subject to constant revision. Unintended consequences, poorly managed risks, and disasters created an anxious public who is unsure of how trusting they should be of scientific expertise (Garland, 2003). Garland (2003, p.76) argues that our relationship with science is more ambivalent than ever before not because of "the risks we face but because of the perceptions and sensibilities we bear upon them." For the most part contemporary society is a society of choices and endless possibilities whereby people who are born into a particular family, in a certain neighbourhood, and who possess a particular job are no longer restrained or defined by these conditions (Garland, 2003). People are freer than ever before to leave their ties to specific communities, people, or circumstances. Things change, people move, identities are no longer static, traditional norms are no longer strictly adhered to and as such people are forced to face risks alone or seek expert opinion which often provides conflicting information. What results is an endemic of insecurity experienced "by well-to-do individuals who are, by historical standards, healthier and more affluent than ever before" (Garland, 2003, p.76). Within the context of the current study, trust in biometric identification technologies is not only an acceptance of the technology but also an acceptance of the creators of the technology, the experts. Moreover, distrust in databases to securely store biometric data translates into a lack of trust in the technology to effectively perform its task and a lack of trust in experts to design a secure system.

The design of the current study did not enable the researcher to probe respondents regarding why they did or did not trust expert systems of identification however, 47% (n=47) of respondents stated that they were 'unsure of the technology' that would be used on finger scan passports while 66% (n=160) of respondents were 'unsure of the technology' that would be used on facial scan passports (as indicated in Table # 6.1). Furthermore, 63% of respondents (n=195) were concerned about breaches to the databases; these same numbers of respondents were also

concerned that biometric data could improperly be used to track people. Individuals who are 'unsure of technology', concerned about data breaches, or fearful of data being used to track people seem to distrust technology as well as the creators of technology. Conversely, the acceptance of and trust in biometric technologies is ultimately a sign of trust in the experts who designed the technology and vice versa.

Looking at the two major themes together (normalizing technology while criticizing experts), it is possible to gain a greater understanding of these issues as a whole. While it has been illustrated that science and technology are increasingly sought during a time when science and experts are facing criticism, the empirical focus of the current study was to examine whether this relationship exists towards biometric passports. As noted above, respondents who felt vulnerable in terms of national security threats were more willing to accept the use of biometric passports. This vulnerability and fear of low probability-high consequence events plays into the increasing use of technological solutions despite their consequences because people are no longer able to manage these global risks alone. People are increasingly willing to give up individual rights in exchange for collective/national security. As depicted in Table #3, 51% of individuals were willing to provide a facial scan to cross international borders while 68% of respondents were willing to provide a finger scan for this same purpose. The acceptance rates for providing biometric data to cross international borders was higher than for any other purpose reiterating the relationship between concerned with national security issues and the acceptance of biometric passports. There was very little acceptance for facial scans on passports therefore no significant factors were found as reasons for acceptance trust however, played an important role in the acceptance of finger scan passports. Individuals who trusted the various biometric technologies were more accepting of finger scan passports as were individuals who were not

concerned with biometric data being used to track people. Trust was also a major factor for individuals who felt the biometric passports could discriminate against various portions of the population. Individuals who feared database breaches or who feared that biometric data would be used to track individuals felt that biometric passports could discriminate against various populations who do not want to submit biometric data for identification purposes. This distrust towards science and experts is, at times, over shadowed by citizens' fears of crime and terrorism and their inability to manage these global risks alone.

6 CONCLUSION & RECOMMENDATIONS

The biometric debate over whether we are entering a 'big brother' like era of control or if the privacy infringing biometric identification systems are simply necessary measures of security to combat crime and terrorism is merely just beginning. We have become increasingly aware of the risks that plague society and as such have become increasingly concentrated in our efforts to manage them (Garland, 2003). Within the field of policing crime has become a technical problem for which predictive calculations and classification profiles are created to manage (Ericson & Haggerty, 1997). Crime is now considered a part of everyday life and is assessed and managed in a similar manner as other routine events such as rush hour traffic (Ericson & Haggerty, 1997). Post 9/11 became an increasingly uncertain time during which, technological systems gained popularity for assessing dangers, ensuring security and monitoring the future (Ceyhan, 2006). Surveillance technologies that were once used to monitor marginalized populations have expanded, subjecting entire populations to increased monitoring (Ceyhan, 2006). Finger and facial scan technologies that were previously used in law enforcement investigations and prison systems, have now entered the commercial and domestic spheres securing items of personal property and restricting access to certain areas (Jain, 2007). While essentially not a new idea, biometric technology within a network society brings forth a plethora of contemporary issues in the realm of risk, many of which will not disappear even after biometric passports are implemented in Canada in 2011.

The notion of 'security' is an abstract concept as it cannot be accurately measured, quantified or even guaranteed. The trade-off between security and fundamental rights is more aptly depicted as a trade-off between an individual's privacy, liberty, dignity, and equality rights for an illusion of security that can never truly be verified. To date, there is no accurate way to

determine how effective our current method of identification is or how effective the future biometric methods of identification will be. For some, it seems as though democratic oversight is diminished in the process of creating technological solutions as the field of scientific expertise is restricted to a small group of individuals often making decisions based on classified information which limits the capacity to anticipate problems and implement effective policies. Privacy advocates argue that security initiatives should not endanger what they were intended to protect whether it be citizens' lives, their rights or the notion of democracy. Conversely, others argue that a broadening of biometric expertise is in fact occurring as legal, social and institutional expertise are sought as are counter experts in non-governmental and non-industrial organizations (Liberatore, 2007).

The current study found that 1) the hypothesized ambivalent relationship people have towards various aspects of scientific expertise is illustrated by the case of University of Ottawa students' perceptions towards biometric passports; 2) the potential discriminatory consequences of biometric passport contributes to this ambivalence and that 3) trust in expert systems is of central importance for the acceptance of biometric passports.

As indicated in Table #1 respondents of the current study expressed various concerns regarding biometric passports including identity theft, cost of technology, abuse of information, and privacy infringements, yet 67% of respondents accept the use of finger scans on passports while only 21% accepted facial scanning. This ambivalence in terms of the variance in the acceptance rates of finger and facial scans as well as the particular reasons why some respondents were accepting of finger and facial scans for certain purposes and not others, needs further examination. The current research study was undertaken as a pilot study to identify some of the general issues surrounding biometrics and to test the current hypotheses regarding the use

of biometrics on passports. The particular data collected for this study highlighted important issues for future debate and enables researchers to have a bit more confidence in the study's hypotheses. The current study was only able to collect data from a small subset of the future users of biometric passports and the study's results reflect that. The current study sample was fairly homogenous in terms of age, educational background, frequency of travel, race and religion. Therefore, a future study is required to expand the current knowledge regarding the reasons associated with the acceptance or non-acceptance of various biometric identifiers amongst a more representative sample of the population. This future study should also probe the nature of trust in experts and systems of technology as the current study identified that 63% of respondents were concerned about data breaches and abuse of information. A study like the one suggested above, would enable a greater understanding of how to build and maintain trust in risk management systems at a time when knowledge is continually changing.

At the present time it seems improbable that a completely accurate system of identification will be implemented in the near future, therefore it becomes important to look into mitigating the discriminatory consequences of biometric identification systems and creating alternate systems of identification for disabled people who cannot put forth a particular biometric identifier. It is often assumed that formal risk profiles are highly effective risk prediction tools however; these formal risk profiles are inherently based upon informal risk profiles of the security related working culture (O'Malley, 2006). Therefore, formal risk profiles are susceptible to producing discriminatory consequences such as false positive identifications and self-fulfilling prophecies (O'Malley, 2006). According to O'Malley, the resort to risk based calculations "is of greater importance ideologically than it is in delivering increased security" as airport security entirely premised upon risk prediction may become less effective than random focused

interdiction (O'Malley, 2006, p.420). Therefore it is imperative that activists and civilians alike continually challenge scientific expertise in order to ensure the continued advancement and improvement of expert systems created to manage risks.

Communication, information and transportation technologies have redefined the boundaries of travel and global relations. The operation of these technologies within a networked society is highly efficient but not without problems. While technological advances ushered in a new way of life these technologies also highlighted the omnipresence of risk and created new risks that are potentially unmanageable with today's technology. This created a heightened fear of crime amongst members of the public as well as anxiety towards expert systems sought to manage risks. An advanced understanding of biometric technologies is confined to small groups of experts who did not have the necessary time post 9/11 to effectively introduce biometric technologies to the public (NSTC, 2008). While it is highly unlikely that any system will ever be able to offer complete security knowledge can be used to minimize and even change risks thus alleviating some of the public's anxiety. Knowledge in the form of education and open debates should be made public to promote more democratic input in order to build trust towards scientific expertise developed behind closed doors (Beck, 1992). While it could be argued that this knowledge may create panic in the public realm it could also be argued that it is better to fear actual risks and known consequences than to fear unknown risks and have anxiety towards the systems that are suppose to manage these risks. Even though knowledge is temporary, continually contested, and often deemed simply the 'best' information to date to manage risks, this democratization of expertise could mitigate fears regarding accountability and bring the biometric debate out into the public forum to more effectively use all available knowledge and

stimulate system improvements. This consultation with non-experts will promote transparency and help establish trust between citizens and the systems that are created to manage them.

Many people are hesitant to trust government agencies and large organizations because they feel that the interests and needs of these institutions are not similar to their own. Therefore, people become skeptical about the information provided by these institutions as well as the competing experts, which makes scientific advice less authoritative. However, it is clear now more than ever, that no one can completely opt out of the network systems that manage contemporary society. The virtual, egalitarian, at times invisible risks that plague modern society cross gender, race, class, religious and cultural boundaries subjecting the entire population to increased surveillance, management and control. In times of uncertainty, trust in faceless commitments becomes an alternative to absolute knowledge wherein the lack of traditional norms brought about a reliance on experts for managing the global risks we can no longer manage ourselves. Even though knowledge is temporary and continually contested it is considered the best information at the present time to offer a sense of security for an uncertain future.

7 BIBLIOGRAPHY

Babbie, E., Halley, F., & Zaino, J. (2003). *Adventures in Social Research: Data Analysis Using SPSS.* USA: Pine Forge Press

Babbie, E., & Benaquisto, L. (2002). *Fundamentals of Social Research.* Canada: Thomson Nelson p. 80-100.

Bachman, R., & Schutt, K. (2003). *The Practice of Research in Criminology and Criminal Jusstice.* 2nd ed. London: Pine Forge Press

Beck, U. (1992). Risk Society: Towards a New Modernity. London: Sage

Beck, U. (1995). *Ecological Politics in an Age of Risk.* Cambridge: Polity Press.

Beck, U. (2002). The Terrorist Threat: World Risk Society Revisited. *Theory, Culture & Society 19* (4), 39-55.

Bell, D. (2005). Biopolitical Strategies of Security: Considerations on Canada's New National Security Policy. *YCISS Working Paper,* 34.

Birch, D. (2002). A World Away From Reality. *The Guardian*, January 24, 2002. Retrieved June 2, 2009 from http://www.guardian.co.uk/technology/2002/jan/24/onlinesupplement

Blanchfeild, M. (2008). Electronic passport will be good for 10 years. *Canwest News Service.* Retrieved March 28, 2008 from http://www.canada.com/topics/travel/story.html

Bureau of Consular Affairs U.S. Department of State. *The U.S. electronic passport.* Retrieved November 2, 2007, from http://travel.state.gov/passport/eppt/eppt_2498.html

Castells, M. (2006). The Network Society: From Knowledge to Policy In M. Castells & G. Cardoso (Eds.), *The Network Society: From Knowledge to Policy.* Washington, DC: Center for Transatlantic Relations.

Castells, M. (2004). Informationalism, networks, and the network society: a theoretical blueprint In M. Castells (Ed.), *The Network Society: A Cross-Cultural Perspective.* London: Edward Elgar, pp. 3-45.

Castells, M. (2001). *The Internet galaxy: Reflections on the Internet, business, and society.* Oxford: Oxford University Press.

Castells, M. (2000). *The rise of the network society.* Oxford, UK: Blackwell.

Castells, M. (1999). *Information technology, globalization, and social development.* United Nations Research Institute for Social Development, Geneva.

Ceyhan, A. (2006). Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics. *Surveillance & Society* 5(2), 102-123.

Current security management and ethical issues of information technology (2003). In Azari R. (Ed.), London: IRM Press.

Douglas, M. (1992). *Risk and Blame: Essays in Cultural Theory.* London:Routledge

Ekberg, M. (2007). The parameters of the risk society. *Current Sociology, 55*(3), 343.

Ericson, R., & Haggerty, K. (1997). *Policing the Risk Society,* University of Toronto Press.

European Digital Rights. (2005). Germany: Biometric Passports In November. *EDRI- gram* July 14. Retrieved October 10, 2007from www.edri.org/edrigram/number3.14/biometrics

Face Recognition. (2008). *Biometric Technology Today, 16*(10), 9-11.

Fleming, S. (2003). Biometrics: Past, Present and Future. In Azari, R. (Ed.), *Current Security management and ethical issues of information technology* (p.111-131). London: IRM Press.

Fumy, W. & Sauerbrey, J. (2006). *Enterprise Security IT Solutions: Concepts, Practical experiences, technologies.* Germany: Publicis Corporate Publishing.

Furnell, S. & Evangelatos, K. (2007). Public awareness and perceptions of biometrics. *Computer Fraud & Security* 1, 8-13.

Garland, D. (2003). The rise of risk In R. Ericson, & A. Doyle (Eds.), *Risk and morality.* Toronto: University of Toronto Press.

Garland, D. (2001). *The Culture of Control: Crime and social order in contemporary society.* Oxford: Oxford University Press.

Giddens, A. (1990). *The Consequences of Modernity.* Cambridge: Polity Press.

Giddens, A. (1996). *In Defense of Sociology: Essays, Interpretations, and Rejoinders.* Cambridge: Polity Press.

Hribernig, G., & Weinzierl, P. (2006). Biometric Authentication. In Fumy, W., & Sauerbrey, J. (eds). *Enterprise Security IT Solutions: Concepts, Practical experiences, technologies* (p.84-102). Germany: Publicis Corporate Publishing.

Jain, A. (2007). Technology: Biometric recognition. *Nature* 449, 38-40.

Larner, W. (2000). Neo-liberalism: Policy, Ideology, Governmentality. *Studies in Political Economy 63.*

Lash, S. (2002). *Critique of information.* Thousand Oaks, California: Sage.

Lee, M. (2001) "The Genesis of the 'Fear of Crime'" *Theoretical Criminology 5*, 4 (467-485).

Leiker, J. (2006) "The Impact of Criminal Victimization on Fear of Crime in Utah" *Paper presented at the annual meeting of the American Society of Criminology (ASC), Los Angeles Convention Center, Los Angeles, CA*, Oct 31, 2006

Liberatore, A. (2007). Balancing Security and Democracy, and the Role of Expertise: Biometrics Politics in the European Union. *European Journal on Criminal Policy and Research,* 13(1-2), 109-137.

Lyon, D (2005). The border is everywhere: ID cards, surveillance and the other in Zureik E, & M. Salter. (Eds.), *Global surveillance and policing: Borders, security, identity* (p. 66-82). Willan Publishing.

Lyon, D. (2006). Airport Screening, Surviellance, and Social Corting: Canadian Responses to 9/11 in Context. *Canadian Journal of Criminology and Criminal Justice* 48(3).

Nanavati, S., Thieme, M., & Nanavati, R. (2002). *Biometrics: Identity verification in a networked world.* New York, NY: Wiley Computer Publishing.

National Science and Technology Council (NSTC) (2006). Biometrics History. Retrieved November 9, 2008 fromhttp://www.biometricscatalog.org/NSTCSubcommittee/ Documents/Biometrics

National Science and Technology Council (NSTC) (2008). Biometrics in Government Post 9/11: Advancing Science, Enhancing Operations. Retrieved November 9, 2008 from http://www.biometrics.gov/Documents/Biometrics

Ng-Kruelle, G., Swatman, P., Hampe, J., & Rebne, D. (2006). Biometrics and E-Identity (E-Passport) in the European Union: End-user perspectives on the adoption of a controversial innovation. *American Journal of Theoretical and Applied Electronic commerce Research* 1 (2), 12-35.

Nugent, J. & Van Daele, Z. (2006). *Taking it to the Streets* Project Report. Retrieved April 10, 2008 from http://www.takingittothestreets.ca/events.html#ProjectReport

Nunnally, J. C. (1978). *Psychometric theory (2nd ed.).* New York: McGraw-Hill.

O'Malley, P. (2004). *Risk, Uncertainty and Government.* London: Glasshouse Press.

O'Malley, P. (2006). Risk, Ethics, and Airport Security. *Canadian Journal of Criminology and Criminal Justice* 48(3) 413.

Palys, T., & Atchison, C. (2008). *Research Decisions: Quantitative and Qualitative Perspectives*. Canada: Thomson Nelson.

Pomerance, R. (2005). Redefining Privacy in the face of new technologies: Data mining and the threat to the "inviolate personality." *Canadian Law Review,* 9(3), 273-295.

Privacy and technologies of identity: A cross-disciplinary conversation (2006). In Strandburg K., Raicu D. (Eds.), United States of America: Springer.

Pratt, J. (1999). Governmentality, Neo-Liberalism and Dangerousness. In R. Smandych, (Ed.) *Governable Places* (p.133-162). Aldershot: Dartmouth.

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

Rose, N. (1996). The death of the social? Re-figuring the territory of government. *Economy and Society 25*(3), 327-356.

Royal society (1992). *Risk: Analysis, Perception, Management.* London: Royal society.

Salter, M. (2003). *Rights of Passage: The Passport in International Relations.* Boulder, CO: Lynne Rienner.

Salter, M. (2004). Passports, Mobility, and Security: How smart can the border be? *International Studies, 5*, 71-91.

Salter, M. (2006). The global visa regime and the political technologies of the international self: Borders, bodies, biopolitics. *Alternatives 31*(2), 167-189.

Solove, D. (2006). The digital person and the future of privacy. In K. Strandburg, & D. Raicu (Eds.), *Privacy and technologies of identity: A cross disciplinary conversation.* United States of America: Springer

Spence, B. (2000). UK Schools Deters Vandals with Fingerprint Technology. *Biometric Technology Today,* 7 (10), 4.

Stalder, F. (2006). *Manuel Castells: The theory of the network society.* Cambridge, UK: Polity Press.

Torpey, J. (2000). *The invention of the passport: Surveillance, citizenship and the state.* New York, NY: Cambridge University Press.

Van Loon, J. (2000). 'Virtual Risks in an Age of Cybernetic Reproduction', in B. Adam, U. Beck and J. van Loon (eds) *The Risk Society and Beyond: Critical Issues for Social Theory.* London: Sage.

Wayman, J., Jain, A., Maltoni, D., & Maio, D. (2005). An Introduction to Biometric Authentication Systems. In J. Wayman, A. Jain, D. Maltoni, & D Maio (eds.), *Biometric Systems: Technology, design, and performance evaluation* (p.1-20).London: Springer.

Weber, L. & Bowling, B. (2008). Valiant beggars and global vagabonds: Select, eject, immobilize. *Theoretical Criminology,* 12(3) 355-375.

Welfare State. (2009). In Encyclopædia Britannica. Retrieved July 21, 2009, from Encyclopædia Britannica Online: http://www.britannica.com/EBchecked/topic/639266/welfare-state

Wells, G. (1996). *Hazard Identification and Risk Assessment.* Rugby: Institute of Chemical Engineers.

Woodward, J. (1998). Biometrics: Identifying law & policy concerns. *Biometrics: Personal identification in networked society.* Yorktown Heights, NY: Kluwer Academic.

Woodward Jr, J., Orlans, N., & Higgins, P. (2003). Biometrics. New York: McGraw-Hill.

Zureik, E. (2004). Governance, Security and Technology: the Case of Biometrics. *Studies in Political Economy* 73, (Spring/Summer).

8 APPENDICES

8.1 Appendix A- Ethics Approval Certificate

Université d'Ottawa University of Ottawa
Service de subventions de recherche et déontologie Research Grants and Ethics Services

August 15, 2008

Michael Kempa
Department of Criminology
University of Ottawa
michael.kempa@uottawa.ca

Jennifer Duff
Department of Criminology
University of Ottawa
jduff047@uottawa.ca

Re: Public Perceptions of Biometric Passports Among English Speaking Students at the University of Ottawa (File # 06-08-05)

Dear Professor Kempa and Ms. Duff,

I am pleased to inform you that Social Sciences and Humanities Research Ethics Board (SSH REB) has now approved your research project. The ethics certificate is therefore enclosed.

During the course of the study, any modifications to the protocol or forms may not be initiated without prior written approval from the REB. You must also promptly notify the REB of any adverse events that may occur.

This certificate of ethical clearance is valid until August 14, 2009. Please submit an annual status report to the Protocol Officer at the latest in August 2009 to either close the file or request a renewal of ethics approval. This document can be found at: http://www.rges.uottawa.ca/ethics/application_dwn.asp

If you have any questions, please do not hesitate to contact me at extension 1787.

Sincerely yours,

Catherine Paquet
Assistant Director (Ethics)
For Peter Beyer, Chair of the SSH REB

550, rue Cumberland 550 Cumberland Street
Ottawa (Ontario) K1N 6N5 Canada Ottawa, Ontario K1N 6N5 Canada
(613) 562 5841 • Téléc./Fax (613) 562 5338
http://www.uottawa.ca/services/research/rge/index.html

8.2 Appendix B- Biometric Passport Questionnaire

Biometric Passport Implementation in Canada Questionnaire

1) Which of the following biometric technologies have you **seen in movies**; which have you **read about**; which have you **used**; and which technologies would you **trust** to accurately identify you: *(Check all that apply)*

	Seen in Movies	Read About	Used	Trust
Iris Scanning	__	__	__	__
Facial Scanning	__	__	__	__
Finger Scanning	__	__	__	__
Voice recognition	__	__	__	__

---

2) For the purpose of identification are you willing to provide: *(please circle responses)*

	A password		A facial scan		A finger scan	
a)To gain access to your workplace	Y	N	Y	N	Y	N
b)To access your personal computer	Y	N	Y	N	Y	N
c)To cross international borders	Y	N	Y	N	Y	N
d)To gain access to health services	Y	N	Y	N	Y	N
e)To make purchases	Y	N	Y	N	Y	N
f)To Access ATMs	Y	N	Y	N	Y	N
g)To obtain a driver's license	Y	N	Y	N	Y	N
h)To vote in elections	Y	N	Y	N	Y	N

---

3) In your opinion, providing **finger scans** for a biometric passport is: *(please circle one response for each question 3a-3g).*

a) A protection of privacy	Neutral	A privacy infringement
b) Convenient	Neutral	Inconvenient
c) An effective security measure	Neutral	Not an effective security measure
d) Necessary	Neutral	Unnecessary
e) Not Invasive	Neutral	Invasive
f) Not an infringement of my rights	Neutral	An infringement of my rights
g) Not a health risk	Neutral	A health risk

---

4) In your opinion, providing **a facial scan** for a biometric passport is: *(please circle one response for each question 4a-4g).*

a)A protection of privacy	Neutral	A privacy infringement
b)Convenient	Neutral	Inconvenient
c)An effective security measure	Neutral	Not an effective security measure
d)Necessary	Neutral	Unnecessary
e) Not Invasive	Neutral	Invasive
f) Not an infringement of my rights	Neutral	An infringement of my rights
g) Not a health risk	Neutral	A health risk

---

5) Would you support the implementation of passports with **finger scans** in Canada?

__No-----→ Why not? *(check all that apply)*

__Privacy concerns __Identity theft __Unsure of technology __High Cost

__Possible abuse of information __Religious views Other(specify)_____

__Yes--→ Why? *(check all that apply)*

__Convenient __Secure __Personal Safety __National Security

__Other(specify)_____

6) Would you support the implementation of passports with **facial scans** in Canada?

__No-----→ Why not? *(check all that apply)*

__Privacy concerns __Identity theft __Unsure of technology __High Cost

__Possible abuse of information __Religious views Other (specify)_____

__Yes--→ Why? *(check all that apply)*

__Convenient __Secure __Personal Safety __National Security

__Other(specify)_____

7a) If passports using **both** finger scans & facial scans are implemented in Canada how concerned are you that databases containing biometric information may be breached?

Very concerned Concerned Neutral Not concerned

7b) Are you concerned that biometric data could be used to track your activities?

Very Concerned Concerned Neutral Not Concerned

For the following statements (questions #8-13) please circle your responses.

8) Canada is:

A very safe place to live A safe place Neutral Unsafe Very Unsafe

---

9) Terrorism in Canada is:

Not a risk Neutral A risk

---

10) The Canadian government effectively addresses national security concerns.

Strongly agree Agree Neutral Disagree Strongly Disagree

---

11) How safe do you perceive Canada's border to be:

Very safe Safe Neutral Not safe Not safe at all

---

12) The Canadian government protects individual rights.

Strongly agree Agree Neutral Disagree Strongly disagree

13) The local police do a good job of ensuring safety in my neighbourhood.

Strongly agree Agree Neutral Disagree Strongly disagree

---

14) In the past five years have you been a victim of: *(check all that apply)*

__ Vandalism (something was damaged)
__ Theft of personal property
__ Break and enter (illegal entry into your residence)
__ Motor vehicle theft/Attempt (theft of motor vehicle or parts)
__ Fraud (including by phone and Internet)
__ Acts of terrorism
__ Assault
__ Robbery
__ Harassment/Stalking (Being the subject of persistent and unwanted attention that caused you to fear for your safety or the safety of someone known to you)
__ Sexual assault (unwanted sexual touching, fondling, rape, and attempted rape)
__ Other not included above *(please specify)*_____

---

15) Please place a check mark in the box that best describes your level of safety when you are **alone during the day** and when you are **alone after dark.**

During the Day	Very Safe	Safe	Unsafe	Very Unsafe
a) In your home				
b) At your workplace				
c) On campus				
d) On foot in parking lots				
e) In public buildings				
f) On a bus				
g) Waiting for a bus				
h) Walking downtown(bordered by *Laurier, Elgin, Wellington, Kent*)				
k) On walking/bike paths				
l) In bars or restaurants				

After Dark	Very Safe	Safe	Unsafe	Very Unsafe
a) In your home				
b) At your workplace				
c) On campus				
d) On foot in parking lots				
e) In public buildings				
f) On a bus				
g) Waiting for a bus				
h) Walking downtown(bordered by *Laurier, Elgin, Wellington, Kent*)				
k) On walking/bike paths				
l) In bars or restaurants				

16) How often do you travel outside of Canada?

__Never __Weekly __Monthly __Once every 6 months

__ Annually __Once in 5 years __Once in 10 years __Other (specify)_____

16 b) Purpose of Travel?

__Primarily Business __Primarily Pleasure __Both Other (specify)_____

---

17) In the past five years have you ever experienced discrimination on the basis of:
(check all that apply)

Age__ Gender__ Ethnicity__ Race__
Language__ Religion__ Disability__ Sexual Orientation__
Other*(please specify)* _____

---

18) Do you feel biometric passports are discriminatory towards:
a) people with religious beliefs who will not submit biometric data for identification purposes?
YES_____ NO_____
b) disabled people who cannot submit biometric data for identification purposes?
YES_____ NO_____
c) others who simply do not want to submit biometric data for identification purposes?
YES_____ NO_____

---

19) When biometric passports are issued in Canada in 2011 what type of legislation would you want implemented: *(circle all that apply)*

a) Legislation to protect your informational privacy to regulate who has access to your data
b) Legislation that gives you the right to know how your biometric data is stored
c) Legislation that states for what specific purpose your biometric data will be collected (to prevent improper use of data)
d) Legislation protecting the rights of religious people
e) Legislation protecting the rights of disabled people
f) No legislation would be necessary
g) Other *(specify)* _____

---

20) Which Canadian political party do you currently support:
NDP___ Liberal ___ Conservative___ The Bloc___ Green Party___
None___ Don`t want to answer___ Other_____

---

21) What is your current age? _____

---

22) Are you Male____ or Female____

---

23) What is your current level of education?

1st year university____ 2nd year university____ 3rd year university____

4th year university____ Masters____ PhD____ __Other (specify)_____

---

24) What faculty are you studying in?

__Faculty of Social Science __Faculty of Engineering __Faculty of Science

__Faculty of Health Sciences __Faculty of Management __Faculty of Arts

---

25) What is your religious affiliation?

__Protestant Christian __ Roman Catholic __Evangelical Christian

__Jewish __Muslim __Hindu

__Buddhist __None __Other (specify)_____

---

26) What is your race?

__White __Aboriginal __Arabic / Middle Eastern

__Black __Asian/Pacific Islander __Other (specify)_____

Thank you for your time and participation.

8.3 Appendix C- Departmental Permission Form

Head of Department Permission Form

Title of the study: Perceptions of Biometric Passports Among English Speaking Students at the University of Ottawa

Researcher
Jennifer Duff
MA Candidate
University of Ottawa
Department of Criminology
25 University St. Ottawa, On. K1N 6N5
jduff047@uottawa.ca

Supervisor
Michael Kempa
Assistant Professor at the University of Ottawa
Department of Criminology
25 University St, Ottawa, On. K1N 6N5
Tel: 613 562-5800 ext. 2572
Michael.kempa@uottawa.ca

I am conducting research for my Master's thesis in the department of criminology at the University of Ottawa under the supervision of Dr. Michael Kempa. Information collected on this questionnaire regarding public perceptions of biometric passports in Canada will provide me with the data that I need to analyze for my thesis and possible subsequent publications in academic peer-reviewed journals after the completion of my Masters. At all times information collected will remain anonymous.

Biometrics is the process of measuring unique physical characteristics such as the retina, fingerprints, voice and hand geometry to establish and verify an individuals' identity. Biometric passports contain a computer chip that stores a digital photograph and the same information visually displayed on the regular photo page of the passport (name, date of birth, gender, place of birth, dates of passport issuance and expiration, and passport number). Fingerprints and/or facial scans are common biometric measures used on passports in many countries. Canada proposed to implement biometric passports by the year 2011. Details have yet to be released regarding what type of biometrics would be included on the Canadian biometric passport. Questionnaire responses will help me gain a greater understanding of how the biometric passport implementation would be received in Canada.

Requesting Permission: I am requesting permission to have access to your department in order to ask professors to gain access to their classrooms so that I can invite students to volunteer to fill out a questionnaire during class. Distributing, explaining, completing, and collecting the questionnaires should take no longer than 30 minutes.

Purpose of the Study: The purpose of this study is to obtain information regarding the public's views towards the use of biometric passports in Canada before the passport program is put into place. This study will examine the acceptance/rejection of biometric passports and determine whether the public's perceptions are in line with governing strategies.

Voluntary: You are under no obligation to allow me access to any course in your department.

Anonymity: Anonymity of the participants will be ensured, as no identifying information will be collected on the questionnaire.

Conservation of data: After I analyze the collected data the questionnaires will be stored under lock and key in my supervisor's office. The data will be stored for a period of 5 years after which time it will be shredded.

Acceptance: I ask that you sign this form to confirm that you have voluntarily agreed to allow Jennifer Duff access to the department mentioned below in order to invite students to participate in her MA research study.

Please keep a copy of this letter for your records.
If you have any questions about the study, please feel free to contact the researcher or her supervisor.

If you have any questions regarding the ethical conduct of this study, please contact the Protocol Officer for Ethics in Research.
University of Ottawa, Tabaret Hall,
550 Cumberland Street, Room 159,
Ottawa, ON K1N 6N5
Tel.: (613) 562-5841
Email: ethics@uottawa.ca

Name of the Chair:_____ Department: _____

Signature: _____ Date: _____

Thank you,
Jennifer Duff
MA Candidate
Department of Criminology, University of Ottawa
25 University St. Ottawa, On K1N 6N5
jduff047@uottawa.ca

8.4 Appendix D- Professor Permission Form

Professor Permission Form

Title of the study: Perceptions of Biometric Passports Among English Speaking Students at the University of Ottawa

Researcher
Jennifer Duff
MA Candidate
University of Ottawa
Department of Criminology
25 University St. Ottawa, On. K1N 6N5
jduff047@uottawa.ca

Supervisor
Michael Kempa
Assistant Professor at the University of Ottawa
Department of Criminology
25 University St, Ottawa, On. K1N 6N5
Tel: 613 562-5800 ext. 2572
Michael.kempa@uottawa.ca

I am conducting research for my Master's thesis in the department of criminology at the University of Ottawa under the supervision of Dr. Michael Kempa. Information collected on this questionnaire regarding public perceptions of biometric passports in Canada will provide me with the data that I need to analyze for my thesis and possible subsequent publications in academic peer-reviewed journals after the completion of my Masters. At all times information collected will remain anonymous.

Biometrics is the process of measuring unique physical characteristics such as the retina, fingerprints, voice and hand geometry to establish and verify an individuals' identity. Biometric passports contain a computer chip that stores a digital photograph and the same information visually displayed on the regular photo page of the passport (name, date of birth, gender, place of birth, dates of passport issuance and expiration, and passport number). Fingerprints and/or facial scans are common biometric measures used on passports in many countries. Canada proposed to implement biometric passports by the year 2011. Details have yet to be released regarding what type of biometrics would be included on the Canadian biometric passport. Questionnaire responses will help me gain a greater understanding of how biometric passport implementation would be received in Canada.

Purpose of the Study: The purpose of this study is to obtain information regarding the public's views towards the use of biometric passports in Canada before the passport program is put into place. This study will examine the acceptance/rejection of biometric passports and determine whether the public's perceptions are in line with governing strategies.

Requesting Permission: I am requesting permission to have access to your classroom in order to invite students to volunteer to fill out a questionnaire during class. Distributing, explaining, completing, and collecting the questionnaires should take no longer than 30 minutes.

Voluntary: You are under no obligation to allow me access to your classroom or your students.

Anonymity: Anonymity of the participants will be ensured, as no identifying information will be collected on the questionnaire.

Conservation of data: After I analyze the collected data the questionnaires will be stored under lock and key in my supervisor's office. The data will be stored for a period of 5 years after which time it will be shredded.

Acceptance: I ask that you sign this form to confirm that you have voluntarily agreed to allow Jennifer Duff access to your classroom in order to invite students to participate in her MA research study.

Please keep a copy of this letter for your records.
If you have any questions about the study, please feel free to contact the researcher or her supervisor.

If you have any questions regarding the ethical conduct of this study, please contact the Protocol Officer for Ethics in Research.
University of Ottawa, Tabaret Hall,
550 Cumberland Street, Room 159,
Ottawa, ON K1N 6N5
Tel.: (613) 562-5841
Email: ethics@uottawa.ca

Name of Professor:_____ Course Code:_____
Professor's signature: _____ Date: _____

Thank you,
Jennifer Duff
MA Candidate
Department of Criminology, University of Ottawa
25 University St. Ottawa, On K1N 6N5
jduff047@uottawa.ca

8.5 Appendix E- Recruitment letter to Participants

Recruitment/Information Letter

Title of the study: Perceptions of Biometric Passports Among English Speaking Students at the University of Ottawa

Researcher
Jennifer Duff
MA Candidate
University of Ottawa
Department of Criminology
25 University St. Ottawa, On. K1N 6N5
Jduff047@uottawa.ca

Supervisor
Michael Kempa
Assistant Professor at the University of Ottawa
Department of Criminology
25 University St, Ottawa, On. K1N 6N5
Tel: 613 562-5800 ext. 2572
Michael.kempa@uottawa.ca

I am conducting research for my Master's thesis in the department of criminology at the University of Ottawa under the supervision of Dr. Michael Kempa. Information collected on this questionnaire regarding public perceptions of biometric passports in Canada will provide me with the data that I need to analyze for my thesis and possible subsequent publications in academic peer-reviewed journals after the completion of my Masters. At all times information collected will remain anonymous.

Biometrics is the process of measuring unique physical characteristics such as the retina, fingerprints, voice and hand geometry to establish and verify an individuals' identity. Biometric passports contain a computer chip that stores a digital photograph and the same information visually displayed on the regular photo page of the passport (name, date of birth, gender, place of birth, dates of passport issuance and expiration, and passport number). Fingerprints and/or facial scans are common biometric measures used on passports in many countries. Canada proposed to implement biometric passports by the year 2011. Details have yet to be released regarding what type of biometrics would be included on the Canadian biometric passport. I ask that you fill out this questionnaire in order to help me gain a greater understanding of how biometric passport implementation would be received in Canada.

Invitation to Participate: You are invited to participate in the abovementioned research study conducted by Jennifer Duff under the supervision of Dr. Michael Kempa of the department of Criminology at the University of Ottawa.

Purpose of the Study: The purpose of this study is to obtain information regarding the public's views towards the use of biometric passports in Canada before the passport program is put into place. This study will examine the acceptance/rejection of biometric passports and determine whether the public's perceptions are in line with governing strategies.

Participation: Your participation will consist of volunteering to fill out a questionnaire. This should take approximately 20 minutes to complete. You will not be compensated for participating however, participation is completely voluntary and all information will remain anonymous.

Risks: There are no foreseeable risks associated with participating in this study. Participants should not expect any risks or discomfort (physical, psychological, emotional, financial and/or social), however in the unlikely event that they do, information about counselling services are listed below.

Benefits: Your participation in this study will provide me with the information I need to conduct my research for my Masters thesis. Your participation will also contribute to the advancement of knowledge regarding how the mandated users of the system perceive the technological solutions that are implemented to govern individuals passing through Canada's borders.

Anonymity: Anonymity of the participants will be ensured as no identifying information will be collected on the questionnaire.

Conservation of data: After I analyze the collected data the questionnaires will be stored under lock and key in my supervisor's office. The data will be stored for a period of 5 years after which time it will be shredded.

Voluntary Participation: You are under no obligation to complete this questionnaire and if you choose to participate, you can withdraw from the study at any time and/or refuse to answer any questions, without suffering any negative consequences. If you choose to withdraw, the researcher will destroy all data gathered promptly after withdrawal.

Acceptance: completion of the questionnaire is taken as consent to participate.

Please keep this information letter for your records.If you have any questions or would like the results of the study, please contact the researcher at the email address provided below.

If you have any questions regarding the ethical conduct of this study, please contact Ethics in Research.
University of Ottawa, Tabaret Hall,
550 Cumberland Street, Room 159,
Ottawa, ON K1N 6N5
Tel.: (613) 562-5841
Email: ethics@uottawa.ca

Thank you for your participation,
Jennifer Duff
MA Candidate
Department of Criminology, University of Ottawa
25 University St. Ottawa, On K1N 6N5
jduff047@uottawa.ca

Resources

Counselling Services
100 Marie-Curie (4th floor) Ottawa, ON
613- 562-5200
couns@uottawa.ca
www.sassuottawa.ca/personal/

Peer Help Centre
85 Universite, Ottawa, ON
613- 562-5249
entraide@uottawa.ca
www.peerhelp.sfuo.ca