THE ANTECEDENTS OF CITIZENS' PRIVACY CONCERNS IN THE CONTEXT OF SURVEILLANCE AND SECURITY MEASURES: A CROSS-NATIONAL ANALYSIS

by

SURAY DUYGULU

A Dissertation submitted to the

Graduate School-Newark

Rutgers, The State University of New Jersey

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

Graduate Program in Global Affairs

written under the direction of

Dr. Norman Samuels: Professor and Provost Emeritus

and approved by

Dr. Yale H. Ferguson

Dr. Gregg G. Van Ryzin

Dr. Osman Dolu

Newark, New Jersey

October, 2016

ABSTRACT OF THE DISSERTATION

The Antecedents of Citizens' Privacy Concerns in the Context of Surveillance and Security Measures: A Cross-national Analysis

By

SURAY DUYUGLU

Dissertation Director:

Dr. Norman Samuels: Professor and Provost Emeritus

By taking into account the debate on the balance between privacy and security (i.e., between security and civil liberties), particularly after the 9/11 terrorist attacks, this study investigates the factors that affect citizens' concerns about privacy across eight countries. In this regard, it examines the impact of mass surveillance on the public. Employing the "Antecedents of Privacy Concerns and Outcomes (APCO) Macro Model," this study attempts to find support for the understudied and tenuous relationship between antecedents and privacy concerns. In addition, it looks at variations between antecedents and concerns across the countries included in the sample. Furthermore, the study raises some questions about the hierarchy of competing rights. The study hypothesizes that citizens' knowledge of laws, perceived type of media coverage, and experience with surveillance measures are positively associated with their privacy concerns, while regime type, terrorism, confidence in government, and privacy regulations are negatively associated with privacy concerns. It applies quantitative research methods by conducting bivariate and multivariate analysis. Results show that experience with surveillance measures increases citizens' privacy concerns, while recent experience with terrorism shifts the focus of citizens towards security, thereby reduces their privacy concerns. In addition, the democracy score of a

country was not found to necessarily explain the intensity of surveillance, quality of privacy regulations, and citizens' confidence in government. The study offers policy implications in terms of balancing competing rights and reducing citizens' privacy concerns. Consequently, it suggests that with technological advances and globalization, the threat of terrorism becomes global, while privacy concerns significantly differs across cultures. Important events do affect the level of concerns.

ACKNOWLEDGMENTS

I would like to thank many individuals whose support was invaluable during the writing of this dissertation and the journey of doctoral work as a whole. First, I would like to express my deepest gratitude to my committee chair, Professor Norman Samuels, who was always reachable, very encouraging, and supportive in this process. As head advisor of this dissertation project, his insights on the dissertation were instrumental. He not only cared about giving good advice to his students about their graduate work, but also cared for his students as individuals. I will always be grateful for this. Thank you, Professor Samuels, for your understanding and sincerity.

At the beginning of this process I had a topic. I knew what I wanted to study and write about, but I fell a little short about how to design my research. At this point I consulted Professor Gregg Van Ryzin. I worked with him on different phases of my research, including data merging, variable formation, and use of statistical software for analysis. He even spent time over the summer answering my questions and checking the accuracy of my statistical analysis. I specifically want to thank for his time and contributions in terms of his survey research expertise.

I would also like to thank Professor Yale Ferguson who agreed to be on my dissertation committee and supported me with his suggestions and global affairs expertise. I attended Professor Yale Ferguson's seminars, the topics of which were very worthwhile, especially one about how to write a dissertation proposal. Later in the dissertation research process, I never missed opportunity to meet with him during his regular visits to DGA.

Special thanks also goes to Professor Osman Dolu. His dissertation, written years ago, was on a similar topic as mine. Therefore, he was very knowledgeable on the topic,

both with respect to theory and methodology. I learned a lot both from his dissertation and publications.

The DGA faculty as well as the DGA administration play an important role in every student's success. I would like to thank Professor Ariane Chebel and Professor Leslie Kennedy. The content of their courses inspired the formulation of my topic. Many thanks to Associate Director Ms. Ann Martin, Director Professor Jean-Marc Coicaud, and Administrative Assistant Ms. Desiree Gordon.

Also, I want to thank my dear colleagues who surrounded me during my graduate studies. In particular, senior TNP officers, Mustafa Demir, Ismail Onat, Esref Erturk, and my friend and TNP cohort, Isa Kagan Karasioglu, as well as an officer junior to me in the TNP but cohort in the DGA, Mehmet Fatih Bastug. I also thank many other colleagues and fellow students not mentioned here who supported me throughout the process.

Special thanks go to my wife, Sinem, and my son, Omer Akif, for their continued and priceless support throughout my graduate studies. They were always patient and sacrificed much time that cannot be recovered.

To Professor Norman Samuels,

My father, Ali and my mother, Vildan,

My wife, Sinem and my son, Omer Akif.

TABLE of CONTENTS

LIST OF TABLES

CHAPTER I

INTRODUCTION

1.1 Importance of the Study

The literature on globalization has long argued that the differences among nations in many faculties of life have eroded under the influence of the phenomenon of globalization. Evidently, globalization operates in different fields such as economy, education, transportation, technology, security, and so on. In this sense, the term global security has drawn attention as a topic to study since many threats transcend the borders of nations, and the adaptations of different nations with respect to global security standards have been seen across continents. After the 9/11 incidents, for example, governments around the world enacted new laws to protect national security, however, these national security regulations have increased citizen concerns about government surveillance, privacy, and the collection of personal information (Solove, 2008).

Similar to global threats, the concept of individual rights have been argued to be universal, if not global. Global security measures are related to civil liberties. Thus, the other side of the coin is the privacy rights of individuals who are living in a global world. As the process of globalization penetrates every field in modern life, it may also be assumed to influence and converge upon the concerns of people in different parts of the world. Surveillance and privacy issues are gaining importance across disciplines and have become highly controversial political issues (Haggerty & Ericson, 2006). Individuals have become deeply concerned about the widespread use of surveillance and collection of personal data (Dinev et al., 2005). The privacy landscape has shifted since the 9/11 attacks (Klosek, 2007). Privacy concerns in the face of security measures in general, and of surveillance in

particular, may also be assumed to be under the influence of globalization. However, few studies have examined whether people in different nations with different levels of threats report the same levels of privacy concerns. Therefore, the understanding of citizen attitudes toward privacy and surveillance is important since public opinion is indispensable to the legislative processes found in different countries (Zureik & Stalker, 2010, as cited in Zureik et al., 2010).

1.2 Statement of the Problem

Modern democratic states have the responsibility of protecting the basic human rights of their citizens. People have a right to be secure from threats such as terrorism, while having the right to privacy as well. Democratic states value the notions of transparency and accountability on the one hand, while they gather personal data with secrecy to ensure the security and safety of people and the state itself on the other. How to achieve the balance between the security and the right to privacy is a puzzle. That balance is expected to be established with the support of appropriate surveillance and privacy laws. While governments want to gather more personal information for security reasons, people demand more privacy. The violations of the right to privacy caused by excess surveillance and the necessity to provide safety and security using surveillance measures seem to be in conflict. The tension between the two can be considered as a social and global problem because many individuals are managing their lives and businesses beyond their countries of origin. In other words governments' national security concerns and other surveillance policies appear to be in conflict with citizens' privacy concerns.

Advance technologies have made it less likely individuals will be left alone and have brought increased concerns about right to privacy as well (Klosek, 2007). Privacy

and data protection have gained social importance as technological advances and data flows play more immense role in shaping the structure of public services. However, what is still lacking in the literature, is an understanding of the public's opinion on privacy and personal data issues, and how people from different countries perceive surveillance (Hallinan, Friedewald, & McCarthy, 2012). An effort to conduct global comparative research on the public's opinion about this matter would contribute to a better understanding of the factors affecting individual privacy concerns, and its relationship with regulations.

1.3 Purpose of the Study

The purpose of the study was to understand the nature of the relationship between privacy concerns of people in different nations with respect to security measures of governments and the antecedents of these concerns. Moreover, investigating relationship between antecedents of privacy concerns and their relations to privacy regulations were among the goals of this study. In addition, this study was interested in exploring how these associations would vary across the eight countries that this study focused on. By studying these relationships, it was hoped a novel contribution to the existing literature would be made.

1.4 Significance of the Study

The current study is significant since, to the knowledge of the researcher, it is the first to extend the analysis of privacy concerns to its antecedents in the public sector rather than the private sector by covering eight different countries.

Previous studies investigating privacy and surveillance issues were mostly carried out in North American context and tended to focus on attitudes toward specific events such as the Snowden revelations (Pew Research Center [PEW], 2014). The scope and sample size of existing multinational studies are limited and their interest is more about privacy concerns over electronic commerce. This study explored cross national variations of privacy concerns and their predictors in eight countries (US, Canada, Brazil, France, Spain, Hungary, Japan, and China). By reviewing 320 articles and 128 books and book sections Smith, Dinev, and Xu (2011) indicate that studies exploring privacy concerns so far are appropriate with their proposed "APCO Macro Model: Antecedents →Privacy Concerns →Outcomes." They state that most of the studies have been interested in the relationship between privacy concerns and outcomes in this sequence of the model. On the other hand a smaller body of research has investigated the antecedents of privacy concerns. Therefore, more data on the relationship between antecedents and privacy concerns is needed and needs to be confirmed through repeated studies. This present study was interested in investigating this relationship in order to make a contribution to the literature.

The link between antecedents and privacy concerns has been studied empirically and descriptively by focusing on individual perceptions. Studies that associated privacy concerns with outcomes have been interested in organizational and societal dynamics (Smith et al., 2011). In addition previous studies mostly made comparisons by taking into account only two countries or regions within these countries. Some of them have already explored the effect of being knowledgeable about the laws, the effect of cultural values, and the effect of perceived media coverage on privacy concerns. The current study included these variables in a regression analysis that was carried out not only for two countries, but

for eight countries that differ with respect to geography, regime or culture. Another difference of the current project from that of the previous literature is that it tested the effects of the variables such as regime, experience with terrorism, and privacy regulations, none of which have been included in the previous models.

In addition, this study combined five different datasets in an attempt to better understand the nature of privacy concerns in the public sector. Previous studies predominantly focused on the private sector, and they used one to three different data points, which limits the explanatory power of the model. Also, the majority of the empirical studies were interested in individual level and private sector analyses. Taking the country context into consideration, this study covers general privacy concerns including a variety of personal data, communication and information privacy concerns. It was specifically focused on citizen's general privacy concerns that stem from governments' national security, surveillance and privacy regulations and policies.

1.5 Globalization and Security

Social control is an aspect of surveillance. In that sense it is also a tool of war-time and peace-time control over threats. Moreover it is a security measure. The understanding of security has changed over time. Some dominant approaches have affected the security concept throughout history. For instance, in 1940s the "Realism" approach was prevalent and security actors were states, and interactions among states were characterized as power politics. The national interest was the first priority issue for security. States did not trust each other and they tried to enhance their military power. When Pluralism was at the forefront in the 1960s the concept of economic power gained importance beside the military power. Also International governmental organizations and multinational

corporations take active role in international politics in power relationships. Until the 1990s, the rivalry between the US and Russian was widespread in all respects. Throughout the bipolar system so-called Cold War time the two countries did not actually attack each other, but they carried out proxy wars by supporting other countries covertly. In that era, intelligence played an important role in both countries. Besides other approaches, Marxism imposed economic concerns rather than military concerns. It advocated the workers dominance over the capitalists and focused on the competition between the wealthy and the poor (Hough, 2008).

After the end of the Cold War the "social constructivism" approach emerged in the 1990s. In this new world order threats have come from sources other than the states. It has been observed that states have been weakened or destroyed by forces other than military conflicts. Some of these non-military threats include terrorism, environmental problems, and societal problems. The understanding of security has changed such that issues can be considered as matters of security even if they are not constituting any threat to a state. Besides the concept of state security, and national security, the concept of human security has emerged. The process of constructive international policy is expected to provide a more comprehensive understanding of security since the emphasis has shifted from national security to the security of the individual citizen. On the other hand, the advance of technology in the latter part of the 20th century has eased the rise of terrorism. The 9/11 terrorists attacks constituted a cornerstone for a new type of security measure (Hough, 2008). The increased use of surveillance technology and the shift in security and surveillance regulations were some of these. Intelligence gathering and surveillance have become one of the state responses to non-state violence. It is stated that wartime measures

significantly differ from those in normal times and extraordinary situations require extraordinary implementations (Solove, 2008). After the 9/11 attacks, the Bush Administration declared a "global war on terror". Since the US was considered to be in a war the use of harsh security policies was justified by the Administration. The public opinion was ready to support these policies in the aftermath of the mass casualties of the attacks.

It is argued that laws of emergency and regulations can be acceptable in emergency situations, however the problem is that they remain effective even after the emergency situations are removed (Solove, 2008). The challenge is that wars between states usually reach a definite conclusion, but wars against non-state actors rarely do (Hough, 2008). Therefore it is not clear whether the terrorists have been defeated or the "global war on terror" has ended. Even though the emergency regulations such as the US Patriot Act were supported by public opinion right after the immediacy of shocking incidents a dilemma between security and civil liberties has emerged overtime.

Civil liberties can be related to human security and societal security. The term societal security is defined as the ability of a society to persist in its essential character under conditions or actual threats (Hough, 2008). These surveillance and national security measures have the potential to harm human and societal security. Legislative texts on human rights and civil liberties include the rights to privacy and protection of personal information. Therefore it can be concluded that right to privacy is related to human security.

Today's world is more culturally integrated then the past. The speed of travel and speed of dissemination of information makes the world globally integrated and interdependent. The events in the one part of the world may impact another. Local incidents have global consequences and international events may have local consequences as well. In other words globalization has led to internal politics that are increasingly externalized and external political issues that are increasingly internalized (Hough, 2008). For instance when the Madrid and London bombings took place, state police in New Jersey took extra precautions in NJ Transit stations and the NYPD increased its security measures in the city's subway system. Another example was that the UN adopted resolutions calling upon all member states to take wide range of measures to fight terrorism (Klosek, 2007). Following the 9/11 terrorist attacks, security measures have been raised to a high level of priority in countries around the world (Lyon, 2007). Those measures include mass surveillance and have been conducted very often under the rhetoric of "national security" and the "common good". However, it is said that with the "national security" pretext many practices are justified, the authorization of safeguards is minimized, and oversight mechanisms are ignored (Privacy International's European Privacy and Human Rights Report [EPHR], 2011).

Technological advances and globalization have not been regarded only from the positive point of view, but they have been criticized. The critics of globalization set forth that after land, sea, air, and space, cyberspace has become warfare's "fifth domain". They argue that by making it possible for terrorists to coordinate through the internet, increasing the porosity of borders, and fostering the illegal transnational illegal trade, globalization facilitates transnational terrorism (Shane, 2010, as cited in Ferguson & Mansbach, 2012).

Thus, the globalization of the terrorism threat has emerged as type of globalization of expectations about possible terrorist attacks almost everywhere in the world at any moment (Beck, 2009). At this point the intelligence community intervenes by means of electronic communication surveillance and that surveillance is regulated by national and international laws. Globalization has led states to realize the adoption of a technology dependent form of governance (Lyon, 2007).

1.6 Globalization and Personal Data Flow

Langhorne (2001) defines globalization as "the latest stage along accumulation of technological advance which has given human beings the ability to conduct their affairs across the world without reference to nationality, government authority, time and day or physical environment." He states that globalization has been made possible by technological advances in global communications. Therefore the communication revolution is the cause of globalization. This concept has two meanings as a process and its consequences. As very early stages of globalization Langhorne (2001) mentions the invention of the printing press. When taken into account as a process, globalization evolved in three stages. The first is the usage of the steam engine and installation of the electric telegraph. The second is the invention of rocket propulsion that led to the ability to develop orbiting satellites. This made possible reliable global communication coverage when combined with the previous invention of the telephone. The third stage constitutes the evolution of the microchip, and the computer and as a result, the internet.

Technological advances are said to be both the cause and consequence of globalization. One technological advance, the internet network, first developed for use by the Pentagon began to be used by the public in 1995 and soon became a global

communication network device for linking business, professional and other services. The internet technology has contributed to the development of new terminology with terms such as “cyberspace”, “electronic highway”, “electronic mail”, “infosphere”, “information technology”, “online community”, and “virtual community”. This technology has enabled fast and instant global communications by mail, fax, cellular and satellite telephones, and the move of money and information with ease. Further, social networks such as Facebook and Twitter provide an opportunity for dispersed national groups to interact and maintain their cultural identities. New communication technologies like smart phones and the internet affect people’s ability to communicate, learn, socialize, produce, sell, consume and to regulate their lives (Ferguson & Mansbach, 2012).

Surveillance is said to be a routine condition that we are all subjected to in our everyday activities of modern society. It is also a global condition, because personal information can now flow freely and instantaneously across digital networks (Bennett, 2008). The personal information that is available over the internet, as well as travel information that can be shared between states, along with economic intelligence information are some examples of the use of transnational dataflow. The governments of many countries demand the sharing of passenger data from other countries. Information sharing demands not only include the public sector, but also the private sector, financial institutions, and even charitable organizations (Klosek, 2007).

1.7 Surveillance

Studies describing and defining surveillance occasionally refer to Foucault’s and Bentham’s propositions about “Panopticon” and Orwell’s “Big Brother”. Jeremy Bentham’s concept of “Panopticon” is described as a prison setting designed around a

central surveillance tower from which the warden could see inside of all cells. In this setting, prisoners have no idea when they are being watched. Foucault used the term "Panopticon to describe how the modern society enforces discipline and control over its citizens. Herein "Pan-" refers to the prisoner while "-opticon" to the guard that monitor behaviors. In his novel "Nineteen Eighty Four" Orwell depicts surveillance of totalitarian states which practice control over personal behavior and thought with the notion of "Big Brother". His argument about the effects of the surveillance on thought and behavior were that the fear of being watched makes people act and think differently from what they might otherwise (Richards, 2013; Fura & Klamberg, 2012; Chesterman, 2010).

Surveillance is carried out for a purpose. In the past it was mostly a tool of totalitarian regimes, but in the modern era, the purpose of surveillance is rarely totalitarian domination. In contrast to "Panopticon", the "Panspectron" the aim is to not only record the visible, but also radio, radar, and microwaves. There is a shift from "Panopticon" to "Panspectron". Most of the current computerized electronic surveillance practices can be considered as forms of "Panspectron" (Fura & Klemberg, 2012).

Surveillance is defined by Clarke (2006) as "the collection and analysis of information about individuals or groups of people in order to govern their activity." Personal and mass surveillance refer to supervision, observation or oversight of behavior through the use of personal data and data systems, by means of physical surveillance, communications surveillance or combined, electronic surveillance (Clarke, 2006). Surveillance is seen as a tool for social control over unwanted behavior. There is an agreement on the notion that every society needs some kind of social control, however the debate is on where to draw the certain line for acceptable social control (Solove, 2008).

With the mass surveillance it becomes so difficult for individuals to keep their identities and many of them are deeply concerned about increased surveillance and individual privacy. Too much social control can harm the citizens' behavior, their freedom, creativity and self-development (Solove, 2006). Therefore, as Goold (2010) argues, when citizens perceive state surveillance as a threat to civil liberties, political rights, and democracy they demand less surveillance. Otherwise they would support surveillance as an effective deterrent to crime and terrorism, which makes it more socially acceptable.

According to Shipler (2011) searching for everyday information about someone's past to predict his/her future behavior may lead to "false positives" and non-compensable mistakes. Even, worse, government authorities with surveillance power may target their political opponents because surveillance technology gives immense power to those who possess it. That power resembles a sword for good or ill and has the potential to both protect and invade simultaneously. Information technology is also used by governments for purposes of social control (Shane, Podesta, & Leone, 2004).

The expression, a "data base nation" by Garfinkel (2000) is consistent with the concept of a "naked crowd" by Rosen (2005). These ideas imply that states possess more information about their citizens than any time before. It is said that much of this information enhances security even though it is difficult to measure. Surveillance is seen among the coercive powers of the state. In addition it generates a debate about what is private information and what is public information. Thus, surveillance is a type of relationship that exists between governments and the governed (Chesterman, 2010). Lyon (2003) points out that modernity and surveillance go hand in hand.

1.8 Privacy

There is no consistent definition of privacy. Even though it is fundamental, it is not an absolute right and needs to be understood in terms of place, politics, and culture (Zureik et al., 2010). Similarly Bennett (2008) sets forth that definitions and concerns about privacy have varied over time and according to national, cultural, and academic perspectives. Pioneers in privacy literature Warren and Brandeis (1890) introduced the concept of privacy as right to be "let alone" and to "keep his/her private life". In the nineteenth century privacy was mostly as the right to be let alone (Klosek, 2007; Solove, 2008). However, the right to be let alone is difficult to define, explain and justify in public policy especially in today's risky society and at a time of terrorism (Shipler, 2011). According to Budak, Anic, and Rajh (2013) privacy is a concept at the interface of surveillance, security, and data protection. Further, privacy is multidimensional concept that tends to define policy issues in advanced industrial societies and challenges the use of excessive surveillance (Bennett, 2008).

There are many definitions concerning the concept of privacy. Westin (1967) defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." In this respect, privacy is regarded as an individual right, as a control over personal data, and as a commodity of the private sector's economic means.

The understanding of privacy was also described by Westin (1967) under four categories, including solitude, intimacy, anonymity, and reserve. First, privacy can be seen as a form of solitude, whereby one is "free from the observation by others." Second, privacy can be understood in terms of intimacy, where there is "small group seclusion for members

to achieve a close, relaxed and frank relationship." Third, privacy can be regarded as anonymity, which allows one to enjoy "freedom from identification and from surveillance in public places and public acts." Last, privacy is set forth by Westin as a form of reserve, or the desire to limit disclosure to others," which "requires others recognize and respect that desire."

Bennett (2008) makes a distinction between the types of privacy such as; the privacy of space, the privacy of behavior, the privacy of decisions, and the privacy of information. The definitions surrounding the concept of information tend therefore to emphasize the importance of "control" or "choice".

Privacy is also categorized as information privacy, bodily privacy, privacy of communications, and territorial privacy. It can be defined as a fundamental, though not absolute, human right (Banisar & Davies, 1999). Another distinction of privacy made by Clarke (2003, as cited in Zureik et al., 2010) is the distinction between behavioral privacy, privacy of person, communication privacy, and privacy of personal data. The concept of "personal data" is defined as "any information that relates to an identified or identifiable natural person (EU Data Protection Directive, 1995)".

Scholars further point out the arguments about the context of privacy issues. For instance Acquisti (2004) argues that privacy should be considered more as a class of multifaceted interests than as a single, unambiguous concept. The value of privacy can be discussed only once its context has also been determined. Some examples for a context could be related to the type or domain of the research construct, time, location, occupation, culture, and rationale (Bansal, Zahedi, & Gefen, 2008). From a different point of view

Smith et al.'s (2011) analysis of privacy research demonstrated that the most often cited contexts for privacy and privacy-related beliefs are: "(1) the type of information collected from individuals (e.g., behavioral, financial, medical, biometric, consumer, biographical); (2) the use of information by sector (e.g., healthcare, marketing, and finance); (3) political context (e.g. law enforcement, constitutional rights of self, government, pubic data and media); and (4) technological applications." In this regard the focus of the study lies more on political context even though it insights are revealed by the remaining contexts.

The political context of privacy is relevant within the US and European legal and constitutional framework. Scholars view the value of general privacy as a necessary one in order to be balanced against other important values including the rights of self, freedom of the press, law and order, and national security (Etzioni, 1999, as cited in Smith et al. 2011). It is argued that most of the literature interested in general privacy issues in political contexts is normative and reflects the authors' strong beliefs (Smith, 2011).

Alderman and Kennedy (1997) state that there is less privacy than there used to be in the past. An intrusion to privacy is deemed justifiable in order to permit the press, the police, and employers do their jobs. It is argued that modern society necessitates a certain loss of privacy and the right to privacy can be exchanged for security to a certain extent. Since privacy does have inherent values we need to minimize the intrusion of privacy (Thesslin, 2011).

The visibility and perceptibility of privacy is emphasized by Szekely (2010, as cited in Zureik et al., 2010). He implies that it is not the violation itself that counts, instead its visibility and perceptibility matters. He introduced the term "threshold of abstraction"

which means the more abstract the violation, the less important it is. Actually we do not know the real level of any privacy intrusion. If we are exposed to surveillance measures and our privacy is violated then we feel and see it. Being a victim of a privacy violation and being exposed to harm that can be observed is relevant to the concept of "threshold of abstraction", because in that respect the threshold is exceeded.

Another perspective of privacy is its acceptance as a human right. The right to privacy is regulated and protected by national and supra-national laws. The intrusion of privacy may include identifying persons' political and religious affiliations, sexual behavior and extramarital affairs, problems with alcohol, drugs or gambling, and their medical condition etc. According to the European Convention of Human Rights (ECHR) Article 8, European Court of Human Rights (ECtHR) ruled that opening and inspection of mail and post, reading telegraphic messages and monitoring and recording telephone conversations are privacy interferences (Fura & Klamberg, 2012).

Richards (as cited in Sarat, 2015, p.34) sets forth that there are four keymyths about privacy. Those claims include, the claim; "(1) Privacy is dead, (2) Young people don't care about privacy, (3) People with nothing to hide, have nothing to fear, and (4) Privacy is bad for business". The author discredits those claims with given explanations and examples and calls them myths. From the perspective of the arts, Shipler (2011) states that privacy is like a poem, a painting or a piece of music and unfortunately, government destroys the inherent poetry of privacy with its snooping. In addition to describing the key factors concerning the topic of privacy, the next sections provides a description of the brief history of privacy and surveillance, in the hope this will contribute to better understanding of these overlapping issues.

1.9 A Brief History of Surveillance and Privacy

The surveillance of communications information is not a new phenomenon. It was already done long before by state officials opening the personal letters of selected individuals in post offices and tapping the land lines of telegraphs and later on the telephone. The use of communication technology has only shifted the manner and scope of these snooping practices. With the onset of globalization, the state surveillance processes have evolved and have been extended to permit the application of global surveillance.

In the American context, it can be said that wiretapping began with the use of the telegraph, going back at least to the American Civil War. The beginning of the 20th century was also the beginning of phone tapping for law enforcement purposes and counterespionage. The "Zimmerman telegram" is an example of the use of an earlier telegraph tapping procedure used for counterespionage purposes. In 1917, that telegram was intercepted, decoded, and passed on to Washington by British. It was a proposal from Wilhelm II's foreign minister to the Mexican government promising that if Mexico allied itself with Germany in case that the United States entered into World War I on the side of Allies, Germany would reward this with the return of formerly held Mexican territory in Texas, New Mexico, and Arizona (S. Taylor, 2014).

With the end of the World War I, the "Black Chamber", a precursor of the NSA, was shut down in order to stop the interception of foreign diplomats' cables in peacetime. However, in the late 1930s, the Army and Navy intelligence officers were decoding diplomatic cables from Tokyo and they found some hints that Japan was preparing to attack the US. However, they failed to connect the dots and prevent Japan's raid on Pearl Harbor. The testing of the atomic bomb in 1949 by the Soviet Union, sooner than the Americans

predicted, was said to be another intelligence failure. Later in 1952 the NSA was created with the intent to eavesdrop on government and their agents in the Communist world and as response to the threat coming from the Cold War (S. Taylor, 2014). Intelligence activities of governments were not only occurring at the international level, but also at the national level.

According to De Rosa (2003) there has always been mistrust against a powerful government in the US. In comparison with the citizens of other countries she argues that Americans are less willing to give access to private information because of this mistrust. They fear that government might abuse their rights if it had information about their activities. This mistrust and fear has some foundations in history. The US government collected vast amounts of personal information including those related to legal and peaceful activities from the late 1930s to the early 1970s. The primary goal of the intelligence agencies was the uncovering of Communist sympathizers during that era. However, they disrupted the legitimate activities of the citizens and organizations.

Privacy protection as a public policy question entered the agendas of advanced industrial states in the late 1960s and 1970s. During these years, there was an abiding assumption that the enactment of a law based on a set of common statutory principles, together with credible oversight and enforcement machinery, was both necessary and sufficient to redress the balance between the vulnerable individual and the power of public and private institutions (Flaherty 1989, as cited in Bennett, 2008).

In the 1960s leaders of the civil right movements had been exposed to excessive surveillance. The well-known case was that which involved the collecting of information

about Martin Luther King's activities. The Watergate Scandal, which erupted in 1972, captured the attention of the public and made its representatives demand an investigation of the past activities of the FBI, CIA, and NSA and other intelligence agencies. The Scandal revealed that the Nixon administration had demanded personal data held by federal intelligence agencies to use against their political opponents. After Nixon resigned from office, Gerald Ford appointed Edward Levi to be the Attorney General. Levi made the FBI to adhere to federal wiretapping laws which had been strengthened in the 1968 Omnibus Crime Control and Safe Streets Act. With the introduction of title III of that Act, the targets of wiretapping had to be informed of surveillance after the expiration of the order. That rule and its enforcement by Justice Department headed by Levi were considered as milestones in the US domestic surveillance policy. To impact on the degree of privacy abuses, the Privacy Act of 1974 was enforced (Rule, 2007).

The intelligence activities that raised public concern investigated later in 1976 by The Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, known as the "Church Committee" was chaired by Senator Frank Church. This committee prepared a report entitled "Intelligence Activities and Rights of Americans" which indicates that intelligence activities conducted in the name of national security often went far beyond what was allowed. Furthermore, the report pointed out the weakness of accountability and control within the system of the intelligence community with regards to the necessity of oversight and supervision (De Rosa, 2003).

The investigation of the Church Committee found that had been illegal wiretapping, bugging, and harassment of American citizens, including government officials, Supreme Court justices, human rights workers, political opponents, and reporters. Among other

findings, the US intelligence community had opened hundreds of thousands of letters, millions of telegrams and created dossiers on hundreds of thousands of citizens. The most notorious case the Committee identified was wiretapping to discredit Martin Luther King with the presumption that he might be a part of a Communist conspiracy (S. Taylor, 2014; De Rosa, 2003).

The Church Committee also identified two important surveillance programs, NSA's SHAMROCK project and the FBI's COINTELPRO program which were scrutinized and seen to have abused their powers. The SHAMROCK program monitored the telegraphic and telephonic data coming into and out of the US for almost 30 years. The senders and recipients of the data, many of them American citizens, were targeted without court orders. The COINTELPRO program was used to disrupt and neutralize individuals and groups perceived to be threats to national security. Information was collected often for political interest. Many aggressive tactics were used under this program which included; inducing employers to fire targets, mailing letters to the spouses of targets to disrupt their marriage, obtaining IRS data and initiating IRS investigations, labeling targets as government informants to make them vulnerable to violence in their organizations, and disseminating misinformation to disrupt demonstrations (S. Taylor, 2014; De Rosa, 2003; Greenwald, 2014). Many of these practices were perceived in government circles as illegal, but it was assumed by the FBI that those activities would be tolerated under the climate of that time (Rule, 2007).

The findings of the Church Committee on foreign surveillance made Congress pass the FISA in 1978, to put a layer of judicial review between the intelligence agencies and their targets. Since then, the FISA has been amended several times, the last one being in

2008 (S. Taylor, 2014). The privacy protections regulated under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 was extended to other communications on the internet domain in 1986 with the Electronic Communications Privacy Act (ECPA) (Rule, 2007). The stance in favor of privacy protections with the restrictions of intelligence activities after the Church Committee investigations continued till 1990s. However, with the end of the Cold War and the emergence of the threat from religious motivated terrorism activities, the priority began to shift in favor of aggressive surveillance. The incidents of the bombing attempts of the World Trade Center in New York in 1993, the destruction of US embassies in Africa in 1998, and the attack on the USS Cole at the harbor in Yemen in October 2000 were linked to the terrorist organization Al Qaeda and muted the past concerns of privacy. With the 9/11 event, the stance was completely changed as far as the direction of security and surveillance processes. Immediately after the attacks, The USA PATRIOT Act entered into force, and this widened the scope of electronic surveillance and other investigative powers (S. Taylor, 2014).

The PATRIOT Act and FISA were amended in 2006 and in 2008. However, they were criticized because they gave broad authority to the intelligence community. After years past since the 9/11 and after the former NSA contractor's revelations on June, 2013 the public has been more inclined to seek privacy than security. When the former NSA analyst Snowden transferred documents to the reporters indicating that the NSA collected bulk information about ordinary citizens, the privacy and security debate arose again, similar to that in the 1970's. Even the US President's addresses to the union included remarks on this topic. In June of 2015, The PATRIOT Act was replaced with the Freedom Act, which reduced the investigative powers of the NSA. However, in the process of

writing of the dissertation two new terrorist attacks took place in the Europe, one in Paris (November 2015) and one in Brussels (March 2016). Therefore, with those terrorist incidents the direction of the citizens' concerns might have shifted one more time.

The evolution of the information privacy concept was described in Smith et al.'s (2011) study. Four periods with their particular characteristics were determined regarding the development process of information privacy. The first period from 1945 to 1960 is called the "privacy baseline" period. There was limited information technology and relatively high trust in government and in the private sector people were not that concerned with information collection. The second period from 1961 to 1979 was regarded as "the first era of contemporary privacy development". During that period information privacy arose as a social, political, and legal issue. The dark side of the technology began to be recognized. The framework of the Fair Information Practices (FIP) act was formulated and the Privacy Act of 1974 was enacted as government regulatory mechanisms. The period from 1980 to 1989 was named the Second Era of Privacy Development. Computer and network systems, database capabilities, federal legislation designed to channel the new technologies into FIP and Privacy Protection Act of 1984 increased in this period. The European countries adopted data protection laws for both public and private sectors. The last period from 1990 to present is the "Third Era of Privacy Development". The characteristics of the Third Era include the increase in the use of the internet and Web 2.0. In addition, the terrorist attacks of the 9/11 changed the information flow landscape and privacy concerns began to be reported as being in the high range (Westin, 2003 as cited in Smith et al., 2011, p. 991).

1.10 Dissertation Organization

This dissertation consists of five chapters including the Introduction, Literature Review, Methodology, Analyses and Findings, and Discussion and Conclusion. In the introduction chapter, I describe the statement of the problem, the significance and purpose of the study and then continue with the terms and concepts that used in the study and touch on issues of globalization, security, data flow and a brief history about surveillance and privacy. In the introduction section I aimed to provide a sense of what this study was about and introduced the topics of security, surveillance and privacy.

The reader can find a broader discussion about the different aspects of the debate about privacy and security in the literature review chapter. Given that the main focus of the study is citizens' privacy concerns, before going to that point the issues around citizen privacy concerns were investigated first and foremost. These issues in the literature include, the justification of mass surveillance, the balance between privacy and security, the actors in the debate such as privacy advocates and intelligence community or law enforcement and their discourses, public opinion, media role, surveillance and privacy laws and regulations, and consequently the propositions about the of citizens' privacy/surveillance concerns and attitudes which are the basis for the later statistical analyses. Prior empirical studies on the subject are also reviewed in this chapter.

Chapter III, the methodology section, includes the research design of the dissertation. I have stated the research questions, hypotheses, data sources, data gathering and merging process with the operationalization of dependent and independent variables, sample and unit of analysis in this chapter. As is understood from the previous sentence, this study uses quantitative techniques. The following Analysis and Findings chapter

includes bivariate and multivariate quantitative analyses of the variables. The relationship between the dependent and independent variables examined and country variations of these were also observed. The findings from these analyses were also stated.

The fifth and the final Discussion and Conclusion Chapter summarizes the findings with the statements of how they relate to the literature. In addition, the limitations of the study, suggestions for the future research and some policy implications are stated.

CHAPTER II

LITERATURE REVIEW

The debate on privacy and security is topical and ongoing. The literature review on this topic shows that researchers mostly depend on public opinion surveys, interviews with authorities from the intelligence community and civil liberty advocates, media content analyses, descriptive studies, and law comparisons for their information. According to Smith et al. (2011) past research examined "the meaning of privacy, general privacy concern, public opinion trends, the impact of surveillance technologies, causes and consequences of privacy protection, consumers' responses to privacy concern, and the need for government surveillance and privacy regulation." On the other hand it is argued that there is little research on the impact of mass surveillance on public and evaluation of the effectiveness of mass surveillance as a counter-terrorism measure. The lack of available data to measure the impact and effectiveness in this regard is the main reason for that. According to Zureik et al. (2010) what the public at large thought of privacy and issues of surveillance was left unexplored. Therefore one of the focus areas in the study explored what at the public at large think about privacy and surveillance. Before examining the issue of citizens' privacy concerns, other shareholders of the debate are investigated. This investigation includes the arguments for both sides of the coin; surveillance supporters and privacy advocates.

2.1 Justification of Mass Surveillance Measures

According to Furedi (2006) we live in "culture of fear" which makes us more vulnerable to perceiving a state of emergency and taking precautions to eliminate these risks. Hoilund, (2010 p.13, 21, 22, as cited in Arndt et al., 2014) discusses the questions

"should we sacrifice parts of our democracy in order to preserve it?" When we feel that we are under threat security becomes the most important goal in society. In a "culture of fear" even small things can be perceived as a threat. This may cause legislation changes and ignorance or negligence of legal rights of citizens such as the right to privacy to maintain security and public order. Changes in legislation under these circumstances are known as "laws of urgency" or "draconian laws". These laws are often put into effect without any broad discussion therefore being lost as a result of contradictions and interference.

Still another justification for the restriction of rights and liberties is explained by the "lesser evil" approach. According to this approach emergency situations can justify the restriction of liberties only if the restrictions or suspensions increase the security level and if they do not impact on the constitutional order in normal time. Since the measures may be problematic and immoral they have to be strictly targeted, used as a last resort, exercised on as small a number of persons as possible, and kept under careful surveillance and control of the democratic institutions (Ignatieff, 2004).

Since there are many ways to obtain biological agents it would be hard to prevent an intended biological attack. Therefore most of the time security risks are perceived as high. When targets are highly vulnerable, and where authorities are unprepared and a variety of weapons are available, the institution of worldwide measures and stopping suspected terrorists before they strike seems so difficult (Garfinkel, 2000). Therefore as Betts (2013) argues the collection, correlation, analysis, and dissemination of relevant information is a vital aspect of national security. He states that governments should collect as much information as possible about threats and opportunities in a timely way for prevention. The power of technology can only be effective with necessary knowledge.

There was criticism concerning the legislative reforms adopted in favor of privacy in 1970s that reduced surveillance capabilities and made a negative impact on the NSA by impeding it from uncovering the 9/11 plot on time. Those who oppose surveillance are blamed for defending terrorists, criminals, and pedophiles (Martin, 2010). Supporters of surveillance policies refer to the information necessary to identify terrorist attacks as a needle in a haystack and stress that more access is better and total access to information is the best. However, even total access may not be enough, therefore additional strategies are needed to connect the dots. Data obtained as a consequence of mass surveillance and intelligence is needed to be stored and analyzed systematically. Further, there must be information sharing among related agencies. The common example for communication failure among first responders is the 9/11 terrorist attack. There were no joint communication channels among first responders at that time. There must be proper information sharing among agencies not only after the incident takes place, but also before it happen. The formation of the Fusion Centers across the US emerged as a solution to the specified need (S. Taylor, 2014).

The fact that criminals and terrorists take advantage of advanced communication technology became prevalent with globalization. In order to detect these individuals and prevent their wrongdoing, state officials are supposed to be at least one step beyond these ‘bad’ guys in terms of tactics and technology. Most of the time terrorists need to communicate in planning and coordination phases of any terrorist attack. Therefore, the best way to detect them before they realize their goals is to intercept their written and spoken communications (Garfinkel, 2000; Fura & Klamberg, 2012).

The huge database under the control of the governments has raised citizens' privacy concerns. A former NSA analyst Brenner puts forward as a counter argument to privacy advocates that "The chance of a citizen's records being scrutinized is infinitesimal, like winning the lottery. Another proposition for the international and state level intelligence is that "everyone is spying on everyone else", even if not on the scale of the NSA. This proposition is more relevant in the context of state level privacy concerns than individual concerns (S. Taylor, 2014).

The actors in the surveillance community rarely talk or do not talk at all. These include law enforcement officials in intelligence agencies, surveillance teams within the companies and their lawyers. If they talk private companies fear scaring away the consumers while intelligence authorities do not want to educate criminals and the public about their capabilities and limitations (Soghoian, 2012). FBI director Comey in his speech at the Brookings Institution argues that encryption technologies may leave the intelligence community in the dark and consequently criminals and terrorists might not be detected. Therefore, he asserts that all private companies should follow some standard rules for responding to data demands. Further, he states that what they are doing in terms of electronic surveillance is lawful. They do not oblige private communication companies to provide them backdoors, instead they access the data when necessary lawfully and by court order. He also adds that he understands the customer and market demands (Comey, 2014; Schwartz, 2008). After the Snowden leaks, companies hardened their encryption processes and reinforced their firewalls. When companies accept the intelligence agencies' demands the concern is that customers might prefer and transfer to those EU companies providing similar services (S. Taylor, 2014).

The intelligence community demands citizens trust in their implementations and should promote the idea that what they are doing is necessary for the wellbeing of the public. The "nothing to hide" argument is a widespread statement in terms of government surveillance discussions as a threat to privacy (Solove, 2007). They say that if you are doing nothing wrong, you have no reason to worry about your personal information and privacy (Shipler, 2011). Several studies investigating citizen attitudes to privacy found that some people are in favor of government regulations and support the nothing to hide argument (Budak et al., 2013).

Another expression put forward by intelligence authorities is that there would be "no privacy without national security". If people are not safe from threats like terrorism they cannot enjoy other rights such as privacy. Therefore security comes first compared to privacy. It is argued that higher levels of concern about security and threat of terrorism in public will be associated with higher levels of government involvement with regulations (Smith, 1994, as cited in Milberg, Burke. Smith, & Kallman, 1995). Emphasizing the priority of security reminds us of the questions "Does mass surveillance keep us safe?" and "Are we safer than before?" Empirically answering these questions would require reaching classified information, which is not easily available to researchers. The actual numbers of plots that the NSA identified and prevented thanks to electronic surveillance are not available to researchers. The information related to prevented cases is not revealed because of the sensitivity of the methods used by terrorists and because of ongoing terrorist threats. However, a former NSA official sets forth that phone records program contributed to eleven cases and one example was the prevention of the incident in which a man attempted to blow up New York City subway in 2009. It is argued that if phone records program was

available in 2001 it might have alerted the 9/11 attacks. Therefore, ending the phone records program could increase people's vulnerability. Inversely, privacy advocates state that the phone records program does not provide unique intelligence and it would have made no difference even if it was available at that time (S. Taylor, 2014).

Others also mention that the actual risk of terrorism and the efficacy of enacted measures are exaggerated (Marmura, as cited in Zuriek et al., 2010). Garfinkel (2000) sets forth that measures taken due to the fear of domestic terrorism have had a significant impact on the lives of citizens. He asks whether these measures had any real effect in reducing the threat. Similarly, Wolfendale (2006) argues that terrorism does not pose a sufficient threat to justify the counterterrorism legislation currently being enacted. Instead many of the current counterterrorism practices pose a greater threat to individual physical security and well-being than non-state terrorism. Ironically she indicated that we should fear counterterrorism more than we fear terrorism.

The main argument behind the justification of surveillance measures is that we live in a risk society and under the threat of terrorism; therefore one of the best measures for counter-terrorism is surveillance. The surveillance technology allows the creation of a global database that can be searched and reached quite easily. However, that the use of mass surveillance has raised the concern of the balance between security and civil liberties.

2.2 Privacy Advocacy

Civil liberty advocates argue that tradeoffs between privacy and security are not necessary (Garfinkel, 2000) and privacy versus security is not a zero sum game (Clarke, 2013). Benjamin Franklin's famous aphorism "Any society that would give up a little

liberty to gain a little security will deserve neither and lose both" is in line with the propositions of privacy advocates. Privacy and civil liberty advocates' views that occasionally appear in news reports have argued that surveillance practices can exceeds the legal limits and they demand all types of surveillance be lawful (Privacy International, 2014). Privacy is considered as a fundamental human right within the scope of civil liberties (Klosek, 2007). It is regulated both in national and international laws. This right is advocated not only by national NGOs but also by international organizations such as the UN. Even though the centers of these international organizations are founded in specific countries such as the US and the UK they operate internationally or at least their focus is global. Organizations such as Human Rights Watch, Freedom House, Amnesty International, American Civil Liberties Union, Electronic Privacy Information Center, Electronic Frontier Foundation, Privacy International, and Liberty are some of these. They challenge government implementations regarding intrusion of privacy. The list of privacy advocacy organizations throughout the world was provided by Bennett (2008) (see Appendix-I).

Besides**,** other international organizations such as the UN release reports on privacy issues. For instance the UN privacy report released on July 2014 supported what the Privacy International had been advocating for so long. The report emphasizes four significant points about privacy. It sets forth the idea that mass surveillance inherently interferes with human rights. Second, mandatory retention of data is neither necessary nor proportionate. Third, there is no persuasive difference between communications content data and traffic data when it comes to privacy. Fourth, states must extend human rights obligations to individuals whose communications pass through their jurisdictions. The UN

report indicates that the states should respect communication privacy if they have control over telecommunication companies or undersea cables pass through their jurisdictions (Nyst, 2014).

The US and UK with their intelligence agencies collecting signal intelligence have a higher capacity of tracking the transnational communications and tapping undersea cables. The NSA and GCHQ have been blamed by privacy advocates for unconstitutional search and seizure. Their concern is that the NSA is "draining the ocean to catch a few fish". When former NSA contractor Edward Snowden disclosed NSA's classified documents in June 2013 those issues began to be discussed publicly. It was said that after the revelations NSA found itself in a "double jeopardy; a rogue behavior in its snooping and incompetence in protecting the information it had collected." The ACLU advocate Jafeer indicated that the NSA abused its power (S.Taylor, 2014). Therefore, the government's interception of communications, physical and transaction surveillance need to be subjected to careful attention and meaningful regulations (Slobogin, 2007).

Another criticism by privacy advocates is that intelligence sharing arrangements fail the test of lawfulness. They argue that secret interpretations of law do not have the necessary qualifications of the law. Secret rules and judicial interpretations have excessive discretion. If people are not able to foresee when they would be affected by interception of their communications, the surveillance law does not have the necessary qualifications of being a law. Botello (2010) emphasizes the fact that generally governments do not explain adequately how they use personal information obtained from citizens.

The UN Office of the High Commissioner for Human Rights' (OHCHR) "The Right to Privacy in the Digital Age Report" dated June 2014 suggests that governments have a positive obligation to protect their own populations from surveillance by foreign entities. In addition, in order to reduce the intrusion of privacy, communication service providers (CSP) who are private sector enterprises should interpret government demands as narrowly as possible. They can evaluate the demand's legal foundation and can do this if court order is present. Further they can inform the customers about the risks and compliance with government demands (Nyst, 2014).

Privacy advocates' ultimate goal is not only to accomplish laws protecting privacy, but they want to keep the debate about privacy alive therefore they believe in that way the protection of privacy will be stronger. They want to raise awareness of people about their rights and organizations about their duties. Looking at the numbers of complaints directed to regulators and subjectively at the types of media coverage in a country may give the idea of ongoing debate about privacy (Privacy International, 2014).

In response to the "nothing to hide", "doing nothing wrong", and "trust to government" arguments of pro-government intelligence community, those who advocate for more privacy ask some critical questions. For instance: "What happens if the government decides the websites you view are wrong or the books you read are wrong?" "Why not accept a policeman in your bedroom, since you are not doing anything wrong?" Still another argument voiced is "Why we use curtains in our windows if we do nothing wrong (Shipler, 2011)?" Solove (2011) refers to the "nothing to hide" argument as a misunderstanding of privacy. He responds to such expressions with questions like "Dou you have curtains?" or "Can I see your last credit card statement"? In this way he implies

that the privacy question is not about hiding things but, about human dignity. Close to his remarks, Garfinkel (2000) asserts that "privacy is not just about hiding things. It's about self-possession, autonomy, and integrity."

Privacy advocates also express their thoughts about the excess use of technology. They argue that unrestrained technology may end privacy. Even though technology by itself does not violate privacy, people and institutions can benefit from technology and their policies can intrude into the area of individual privacy. Technological advances have made data flow centralized and easier, therefore, the control of data shifts to fewer people. The centralization of personal information has raised the concern of being the seeds of some future totalitarian regimes (Garfinkel, 2000). For instance five English speaking countries, the so called "Five Eyes" have built an alliance and a global surveillance infrastructure to monitor the internet and spy on the world's communications (Privacy International, 2014).

In a documentary film by Laura Poitras (2015) "Citizenfour", Glenn Greenwald one of the journalists who reported the Snowden leaks argued that governments emphasize terrorism, national security, and criminal investigations as a reason for mass surveillance. However, he added that this was not the case. The intelligence community's surveillance aims at obtaining rival non-US companies' sensitive information, economic assets information, and spying on foreign governments (Poitras, 2015).

Even though privacy advocates and intelligence community have different thoughts on privacy and security they agree on the necessity of clearer regulation, more transparency and accountability is possibly needed (Thesslin, 2011; S. Taylor, 2014).

One of the privacy advocacy organizations, Privacy International briefly described what kind of world they want to see in terms of surveillance and privacy with the following words: "We would like to see a world where surveillance is minimized, conducted under law, only when necessary in a democratic society, and proportionate, with appropriate inbuilt safeguards, and rights of recourse (Privacy International, 2014)." The central privacy-security equilibrium considered as foundation of democratic civil liberties. Countries are expected to take significant steps towards equilibrium (Soma, Nichols, Rynerson, & Maish, 2005).

Table 2.1. Comparison Table of Pro-Surveillance and Pro-Privacy Arguments

	Pro- Surveillance	Pro-Privacy
Surveillance and data collection	The more data is better, Needle in a haystack argument, Nothing to hide argument	Call for minimization, Draining the ocean to catch a few fish, When necessary in a democratic society, Proportionate, It is not about hiding things but dignity, self-possession, autonomy, and integrity
Risk of terrorism, National security	Measures are needed and effective to prevent and preempt terrorism threat	Exaggerated, Gap between perceived threat and actual threat, Economic and diplomatic snooping
Surveillance Practices' Lawfulness	Everything done is lawful	Abuse of power, Exceed the limit of lawfulness
Privacy v. Security	More security –less privacy, Zero-sum game	Trade off not necessary, Not a zero-sum game, Equilibrium, Maximum of both
Trust	Trust in government, Trust in LEA	It is not about the trust but law
Regulations	*Clearer regulations, Accountability, and Transparency*	*Clearer regulations, Accountability, and Transparency*

2.3 Media Coverage

One of the most important forces shaping public opinion is the media (Marmura, 2010). Public attitudes toward key issues have been influenced by media coverage (Zureik

and Stalker, 2010) and privacy issues are often linked to security in the context of policy and media discourse (Zuriek et al., 2010). Investigating what is researched on the topic, it is possible to find various media content or discourse analysis studies. For instance Barnard-Wills' (2011) study drawing upon Neuman, Just, and Crigler's (1992) five media frames, investigated the discourse of the British newspaper articles between 1991-2008 whether they presented the topic of surveillance as appropriate and positive or inappropriate and negative. Although this researcher found more than thousand articles benefitting from a broad Lexis-Nexis search, the author lowered the sample to 300 articles. Barnard-Wills (2011, p.555) summarized the positive and negative media discourses using the following table;

Table 2.2. The Assessment of Surveillance according to Five Media Frames, according to the Table Adopted from Barnard-Wills' (2011, p.555) Study

Frame	Positive	Negative
Economic Issues	Spending on surveillance as attention to problem	Spending as waste inappropriate burden of cost Surveillance industry
Human Impact	Saved by surveillance, Failed by lack of surveillance	Victims of surveillance Exposure, harm, and privacy
"Them" and "us" divisions	Surveillance as safety and security, Crime reduction	Inappropriate subjects of surveillance, Mass rather than targeted, "Us surveilled by "them"
Control by powerful others	Surveillance is not social control, Paranoia of critics	Big Brother, Totalitarian, Surveillance society
Moral values	Crime prevention, Risk management Protection of vulnerable, Moral need for more surveillance	Privacy, Accountability, Democracy

Haggerty and Gazso (2005) published another media study. In that study they examined two newspapers, The New York Times and The Toronto Globe and Mail, for a

three month period following the 9/11 incident. Hundreds of articles regarding surveillance were collected. They looked for surveillance powers which were available to authorities at that time to track the terrorists and in the aftermath of the attacks what proposals were set forth in order to prevent future terrorist plots. To identify future surveillance proposals they used four categories: documentation, visualization, integration (cooperation) and "other." Using a similar method it would be possible to conduct research on different newspapers and in various countries taking into account different terrorist incidents such as the London bombings in the UK and the Madrid bombings in Spain. Haggerty and Gazso (2005, p.173) found that the following forms of surveillance were available to authorities at the time of the 9/11 attacks;

Table 2.3. Available Surveillance Forms at the Time of 9/11

Air Traffic Control	Pilot's License
Airline Flight Records	Parole Records
Arrest Warrants (outstanding)	Passport
Automobile Registration	Personal Computer Records (suspected terrorists)
Automobile Rental Records	Photo Identification Card
Automobile Financing Records	Radar Tapes
Bank Records	Refugee Claims
Black Box (airplane)	Rent Subsidy Cheques
Credit Card Records	Securities and Exchange Trading Records
Criminal Records	Student Records
DNA (recovered from crash sites)	Surveillance Camera tapes (airport, banks, E-mail Logs etc.)
Driving Records (i.e. speeding tickets)	Taxi License
Driver's License	Telephone Logs
Employment Records	Telephone Numbers
Fingerprint Records	Transponders (airplane)
Ferry Records	Vehicle Registration
Flight School Records	Video Footage
Forensic Evidence	Visa (records, applications)
Hotel Booking Records	Wedding Photographs
Immigration Files	Wiretaps
Intelligence Databases	
Mailbox Rental Records	
Medical Records	

Besides the availability of certain surveillance forms, The New York Times and The Toronto Globe and Mail newspapers published articles for three month after the 9/11 attacks that included suggestions for equipping the intelligence authorities with very broad surveillance capacities. The realization of these proposals would require entry of some new legislation into force (Haggerty & Gazso, 2005, pp.175-177).

Gerbner's (1998) "Cultivation Theory" research compares light, moderate, and heavy television viewers. The author proposes that heavy viewers are generally more likely to perceive the world as a dangerous and violent place than light and moderate viewers. They develop unrealistic fears about threats to their safety. The theory sets forth that harsh law enforcement policies tend to be perceived as necessary for the maintenance of public order and security by heavy television viewers.

According to Zureik (2010) the American public has seen the media pay more attention to the root causes of terrorism. Although there has been a decline in public support of intrusive surveillance measures since 2001, Marmura (2010) argues that a substantial public tolerance for government privacy violations still remains due to the media. Contrary to this view it can be expected that if the media covered more stories about government privacy violations and the legal rights about privacy, citizens would not tolerate surveillance measures. The quality and the quantity of media news and reports may influence public attitudes.

Ceyhan (2010) introduces research concerning privacy and surveillance developments in France. After the 9/11 process France adopted a "layered security" approach and invested in security and antiterrorism technologies. Ceyhan states that France

and Hungary appear in the Globalization of Personal Data (GPD) survey as countries least likely to feel laws aimed at protecting national security are intrusive to personal privacy. The relatively lower level privacy concerns of French citizens are explained by their experience with terrorism and media coverage. France experienced Middle Eastern based terrorist attacks in 1980s and Algeria related terrorist attacks in 1990s. Therefore terrorism and security issues receive more media attention rather than coverage about privacy and personal information.

2.4 Public Opinion Polls

Public opinion polls are generally taken into account for purposes of policy formation by governments (Weissberg, 2001). It is said that understanding public opinion is integral to modern democracies. It helps politicians to connect with citizens, and reveals most important issues that are then contemplated by political decision-makers (Carballo & Hjelmar, 2008).

There are many public opinion surveys focused on the relationship between privacy and security measures. To examine what citizens in a country think about specific issues, research companies have taken nationally representative samples and used questionnaires. However, public opinion results have not remained stable. They vary depending on how the question is asked. Moreover, public opinion is affected by important events and it changes over time. Supporting this argument, former National Security Council aide and political science professor Peter Feaver indicates that if public perceive imminent threat, they are more eager to value security rather than privacy and liberties. But, when the threats seem more remote the concern shifts in the opposite direction (Page, 2014). For instance The Patriot Act received near unanimous votes in congress and public opinion polls

reflected overwhelming support. However, that support both on Capitol Hill and among the public changed over time from the 9/11 to the Snowden leaks period (S.Taylor, 2014). Supporting the fact that public opinion changes over time, Davis and Silver (2004) found that the greater people's perception of threat, the lower their support for civil liberties. However, this impact interacts with trust in government.

Public opinion polls examined citizen attitudes to anti-terrorism legislation have focused on privacy in the context of national security (Zureik, 2004). For instance the Queens University's Surveillance Studies Center provides survey data which includes citizen attitudes toward privacy and surveillance as conveyed first in 2006 in nine countries (Ipsos Reid, 2006), and later in three countries using different questionnaires as follow-up surveys in 2012 and 2014. Although the questionnaires were different there were a few similar questions regarding the use of government surveillance measures in the US and Canada. The two countries are similar and the question that was asking the public opinion about government enacted security laws' intrusiveness was the same in all three surveys. Therefore, it is possible to follow if privacy concerns changed over time. Table 2.4 illustrates the shift over time in privacy concerns in regards to government surveillance laws:

Table 2.4. Total percentage of highly intrusive and somewhat intrusive answers to the question "The government of ... has enacted laws aimed at protecting national security. To what extent do you believe laws aimed at protecting national security are intrusive upon personal privacy?" in two countries:

SURVEY	YEAR	QUESTION	COUNTRY	PERCENT	SAMPLE SIZE
GPD survey	2006	q.17	US	57.22 %	1000
Follow-up 2012	2012	q.9	US	63.00 %	1002
Follow-up 2014	2014	q.1	US	67.00 %	1017

SURVEY	YEAR	QUESTION	COUNTRY	PERCENT	SAMPLE SIZE
GPD survey	2006	q.17	Canada	47.70 %	1001
Follow-up 2012	2012	q.9	Canada	60.00 %	1001
Follow-up 2014	2014	q.1	Canada	64.00 %	1502

Source: Queens University Surveillance Studies Center's Survey Archive

Survey results in both countries strengthen the proposition that if the public does not perceive an imminent threat and thinks that the risk is remote, their support for national security laws will be lower and they will be more concerned about their privacy. Furthermore, it can be concluded that important events such as the Watergate Scandal, 9/11 terrorist attacks, and whistleblowers' (e.g. Snowden) revelations may affect the level of citizens' privacy concerns.

A summer 2013 poll by the PEW Research Center revealed that for the first time in a decade a majority of Americans were more concerned about the government infringing their civil liberties than about potential terrorist attacks (S. Taylor, 2014). Similar results

were found by a Gallup poll survey conducted on June 10-11, 2013. The Gallup poll was measuring the support for a government program that obtained records from larger US telephone and internet companies in order to create a database. As parts of its efforts to investigate terrorism, the federal government agency program was disapproved of by 53% of respondents, while it was approved by 37%. Besides, 35% percent of Americans were very concerned about violations of their privacy rights. These results came after the whistleblower Snowden's revelations were first published on June 5, 2013 (Newport, 2013). According to Clarke (2013) the momentum is on the side of greater privacy protections as of 2013. However, in the time frame of completing this study two European capitals Paris and Brussels have been targeted by terrorist attacks. Experiencing these attacks has the potential to shift the momentum.

The comparative survey of the GPD Project conveyed to over 8,000 individuals in nine countries (Canada, United States, Mexico, Brazil, France, Hungary, Spain, Japan, and China) found that respondents in these countries believed their governments had not struck the right balance in protecting their security and privacy. The results of the survey led to the views that governments may undermine privacy interests by a combination of legal reforms and powerful surveillance technologies (Ipsos Reid, 2006).

Another Pew Research Center's comprehensive survey examining global attitudes asked 48,643 respondents in 44 countries what they thought about the US government's surveillance of their phone and internet communications, along with monitoring of others. The questionnaire was seeking respondents' opinion about whether they find the US strategy of monitoring their own country citizens, monitoring US citizens, monitoring their leaders, and monitoring the terrorist suspects acceptable or unacceptable. The median

percentage of the responses reflected that the majority of respondents found monitoring their own country citizens, the US citizens, and their country leaders unacceptable while they assessed monitoring phone and internet communications of the terrorist suspects acceptable (PEW, 2014).

Table 2.5. Median percentages across 43 countries saying it is acceptable or unacceptable for the US government to monitor the communications of survey country citizens/survey country leaders/American citizens/suspected terrorists

US Monitoring _	Unacceptable	Acceptable
Survey Country Citizens	81%	12%
Survey country Leaders	73%	20%
American Citizens	62%	31%
Suspected Terrorists	29%	64%

Note: Global medians exclude the US; Source: Pew Research Center's spring 2014 Global Attitudes survey. Results released on July 14th, 2014.

The PEW survey report released on March 2015 demonstrates Americans' privacy strategies after the Snowden revelations. A survey conducted on a sample of 475 American adults asked what they thought of the government's surveillance programs, the way programs were run and monitored, and whether they had altered citizens' communication habits and online activities since they learned about the details of the government surveillance. The study demonstrated the extent of the privacy concerns of citizens and the impact of surveillance programs on them. The results also revealed how citizens responded to programs and who they thought should be targets of surveillance. About 87% of these respondents had heard at least something about the programs. Among those who were aware of the programs 34% had taken at least one step to hide their information from the

government. Those steps included changing the privacy setting on social media (17%), using social medial less often (15%), avoiding certain applications (15%), uninstalling applications (13%), speaking more in person (14%), and avoiding the use of certain terms in online communications. These steps were taken as evidence that citizens continue to have concerns about their privacy and the steps taken can be considered as outcomes of their privacy concerns (Rainie & Madden, 2015).

Citizens who heard a lot about the surveillance programs and those who said they were less confident that programs were in public interest were more likely to take protective steps. These results showed that awareness and concern were predictive of reactionary outcomes. Younger adults under the age of 50 (40%) were more likely than those ages 50 and older (27%) to have changed at least one of these behaviors. Results supported the view that elderly people have less concern about privacy and surveillance. In addition, 25% of the respondents who were aware of the surveillance program had changed their own use of various platforms since the Snowden revelations. Changes include the way they use email, search engines, social media sites and cell phones. They also used more complex passwords. The majority of the respondents were not aware of tools such as email encryption programs like "Pretty Good Privacy (PGP)", "DoNotTrackMe" or "Privacy Badger", proxy servers that could help them avoid surveillance, and anonymity software such as "Tor". Sixty six percent of the respondents were less than confident the surveillance programs were serving the public interest (Rainie & Madden, 2015).

Citizens were also found divided on the view as to whether judges are balancing the needs of law enforcement and intelligence agencies with the citizen's right to privacy

(48% balance exist, 49% no balance). A high majority of respondents (82%) find monitoring of suspected terrorists by government acceptable. They also approve the monitoring of foreign citizens (54%), foreign leaders (60%), and American leaders (60%) while disapprove of the monitoring of American citizens (57%). If words like "explosives" and "automatic weapons" are used in the search engines the majority of respondents (65%) agree that those need to be monitored. Survey results further showed that 52% of the respondents were very concerned or somewhat concerned about government's data and electronic communication surveillance. Respondents expressed lower levels of concern about their own communication and online activities compared to general questions (Rainie & Madden, 2015).

Survey responses measuring the public attitudes may be strongly influenced by how survey designers utilize the terms such as "trust", "mistrust", and "confidence". Moreover, poll results may be influenced by particular institutions, branches, policies, politicians, or incidents that respondents may have foremost on their minds at the time of the interview (Marmura, 2010, p.117).

Since the wording of survey questions can affect the survey results, the Pew Research Center conducted a research study to examine if differences would be observed when certain words were included or not in the questions. Measuring the public's opinion on government surveillance, it was observed that general questions gave different results when compared to the when the form of questions included the terms terrorism, court order, metadata or content data. If the phrases "counter terrorism" and "court approval" were included in the questions the approval rate for government surveillance program increased, if not, the approval rate decreased (PEW, 2013).

Table 2.6. The Effect of Wording on Survey Results about Government Surveillance

Survey Question: Thinking about the debate over the US government's surveillance programs, would you favor or oppose the government…			
Mention of courts	Favor%	Oppose%	Don't Know%
…data collection "with court approval"?	37	56	7
...data collection? (No mention of courts)	25	67	8
Difference	*+12*	*-11*	
Mention of terrorism	Favor%	Oppose%	Don't Know%
…data collection "as part of anti-terrorism efforts?"	35	57	8
...data collection? (No mention of terrorism)	26	67	7
Difference	*+9*	*-10*	

Source: PEW Research Center July 11-21, 2013

Besides the wording of the survey questions, respondents' statements may mislead the survey results. Researchers point to the challenge of "privacy paradox". Responding to public opinion surveys, individuals state their privacy concerns, but they may behave differently from what they stated they would do. Most of the time studies measure the stated intentions instead of actual behaviors. This is regarded as the privacy paradox (Norberg, Horne, & Horne, 2007; Nissenbaum, 2009).

Budak et al. (2013) indicated that public opinion on surveillance can vary depending on the instruments used by states for surveillance. Citizens living in countries with higher developmental level in terms of technology and citizens living in

underdeveloped countries dealing with economic issues may reflect different levels of concern about the issues of surveillance and privacy.

2.5 Public Opinion and Public Policy

Reviewing the recent public opinion polls can make one wonder to what extent public preferences are taken into account in policy-formation. At least since Jean-Jacques Rousseau's "The Social Contract (1762)" the relationship between public opinion and policy has been the central concern of the literature on representative democracy.

Mainly there are three different views about public opinion. The first group of authors express serious reservations about the potential of the average citizen to make any contribution to the function of government. A second group sets forth that even though the public has little to contribute to government, elected leaders cannot afford to ignore their views. The third group of philosophers supports the idea that public opinion has a critical role to play in democratic societies In other words the first group views citizen opinions as undesirable and unnecessary, the second group views citizens' involvement as undesirable, but necessary. And the final group views citizen engagement as both desirable and necessary. According to the populist perspective, public opinion research has an important role to play in democratic societies because it provides the means for the public to participate and influence government (Ferguson, 2000).

Social constructionist perspectives argue that public opinion is malleable and subject to manipulation. According to the critical perspective of mass public opinion, this is considered as an elite opinion because elites together with the government manipulate the polls to achieve their goals (Ferguson, 2000).

Soroka and Wleizen (2009) developed a model to empirically test the opinion-policy relationship. This so-called "thermostatic model" is used with reference to the home temperature control system, where the public is the thermostat and policymakers are the furnace of air conditioning unit. If their model works they expect to observe three things. First, the difference between the desired temperature and the actual temperature would cause the public to send a signal to change the policy temperature. For instance a signal could be sent to increase the heat. Second, in response to the signal, policymakers could alter the policy. Third, as the policy temperature comes close to the desired temperature, the signal for change would be reduced. The described process is authors' expectation about how the democracy should work. These authors seek to answer the questions: "Do policymakers respond to public preference signals? and "Does the public adjust its signals in response to what policymakers do?" Government regulations about privacy and surveillance as well as policy may influence privacy concerns. Therefore, the public may send signals including their concerns to the legislative branch and later the legislative branch may adjust its policies or may not adjust these.

Soroka and Wleizen (2009) remain doubtful about the policymaker's use of polls. However, they say that they are not interested in knowing to what extent politicians actually use polls, instead they are interested in policymakers' responsiveness to public opinion. They make a distinction between the polls and public opinion by stating that polls provide information about public opinion, but they are not the same. Consequently they state that politicians generally do not follow the polls in decision making but they do follow public opinion. If there is no public responsiveness to policy, there would be little reason for policy responsiveness to public opinion. They put forward that the thermostatic model is

not as demanding for the people. Citizens are not expected to know every regulation and action of policymakers. Not all of them are expected to respond. If a meaningful proportion of the public has a preference for policy change and they adjust this over time in reaction to policymakers' acts based on information they receive from mass media, political groups, family and friends, and daily experiences with government services and society, this would be enough. Authors believe that under certain circumstances, both public and policy responsiveness are possible and they may change across domains and countries.

2.6 Attitudes toward Privacy and Surveillance and Citizens' Privacy Concerns

The systematic analysis of empirical studies employed in to examine public opinion about privacy and surveillance dates back to the mid-1970s (Katz & Tassone, 1990, as cited in Zuriek et al., 2010). The majority of this literature has focused on the US. The lower level of focus on privacy and surveillance issues in other countries may be due to the varying legal environments. Smith et al. (2011) indicate that more research focusing on international dimensions of privacy is needed.

In terms of privacy concerns and attitudes toward privacy and security Haggerty and Gazso (2005) point out two groups of citizens. Those consist of individuals concerned about increasing surveillance or reduced privacy rights, and citizens who can be designated as being "pro-surveillance oriented. In addition there may be groups with different attitudes toward surveillance and privacy. In a similar way Equifax's 1991 public opinion survey on privacy in the US observed three groups of citizens. First, "privacy fundamentalists" who were highly concerned group of respondents, second "the pragmatic majority' were citizens with moderate concerns, and third "the unconcerned" were citizens with low

privacy concern (Gandy, 2003). Categorization of these three groups of citizens were based on the Harris-Westin Index of General Privacy Concern.

Harris-Westin's (1991) "Index of General Concern about Privacy" consists of four items. One specific response indicating high concern is used for each item. One of the questions asks respondents if they feel a threat to their personal privacy. The second question asks whether consumers have lost control over personal information. The third question asks if respondents agree that business organizations seek exclusively personal information from consumers. The fourth question asks if they think that federal government since Watergate scandal is still intruding personal privacy. Respondents are classified in three categories as high, moderate, and low concern respondents according to their responses to the four survey questions. If they express high concern on three or four of the questions, respondents are categorized as being in the high concern category, also called "privacy fundamentalists". If they state high concern on two or three of the questions, the respondents are placed in to a moderate concern category called "privacy pragmatists". If they respond to one or none of the questions with a high degree of concern, they fall into the low concern category, which is also called the 'privacy unconcerned" category. The privacy fundamentalists reject all arguments that favor surveillance and societal-protection claims for data use and they want more regulatory privacy measures. On the contrary the privacy unconcerned citizens are ready to provide their information to authorities and do not accept that there is too much privacy violation. The privacy pragmatists who are moderate concern group evaluate the benefits and risks of personal information collection to them or society and then they decide whether to trust or seek legal regulation and oversight (Westin, 2003, as cited in Zureik et al. 2010).

Smith (2006, as cited in Zureik et al., 2010) and Margulis, Pope, & Lowen (2010) found the GPD survey questions compatible with the questions of Harris & Westin's (1991) index of general privacy concerns. They used one or more questions from the GPD survey for each four categories of Harris-Westin's privacy concern index. Similarly this study followed the same method taking some questions used by prior scholars to form the privacy concern variable. The questions from the GPD survey that they considered compatible and the current study's questions that constituted the dependent variable are shown in the table below. Questions 2 and 11 were discarded after the reliability test was conducted, and this is explained in detail in the methodology chapter.

Table 2.7. Comparison of Questions Taken Concerning Privacy Concerns

Harris-Westin	Smith (2006)	Margulis et al. (2010)	This study
Concern about threats to your personal privacy	**11**	6, 10, **11**	10,**11** (discarded)
Consumers have lost all control	**2**	**2**	**2** (discarded)
Business organizations seek exclusively personal information from consumers	6, **19**	**19**	**19**
Government still invading citizen's privacy	**5, 17, 18**	**5, 17, 18**, 23	**5,17,18**,23

Source: Zureik et al. (2010, p.94)

Budak et al.'s (2013) recent study investigates public attitudes towards privacy, data protection, surveillance, and security in Croatia. Their public opinion survey measures how individuals value the concept of privacy and whether privacy is recognized as a social and political value. Their study covered questions about privacy violations including information collection, information processing, information dissemination, and invasion.

Their empirical research aimed to classify citizens according to their attitudes and they assumed that some groups of citizens sharing similar attitudes differ according to their demographic characteristics. Results show that younger people are using more technology and they are more aware of data protection risks, whereas elderly people in Croatia are more pro-surveillance and support the "nothing to hide" approach. On the other hand the level of education, income, and social status were found to be positively related with privacy concerns. Higher status groups generally criticize state policies more vocally than those in the the lower status groups (Budak et al., 2013), and college graduates show more support for individual rights and civil liberties (Davis & Silver, 2004). Perception and responses of surveillance may also vary across class and gender however this is said to be an under researched area.

Other scholars Zureik and Stalker (2010) were interested in examining demographic variables in cross-national surveys. They argued that very few studies on privacy have implemented cross-national comparisons by using age, gender, race, income, and education as variables. They wondered whether cross-national variations would remain when controlling for demographic variables. One of the previous studies had already investigated the relationship between demographic differences and privacy concerns and found that women are generally more concerned than men about the surveillance and privacy (Sheehan, 1999, as cited in Smith et al., 2011). In addition it was found that being young, poor, less educated, and African-American was associated with a lower level concern about privacy (Culnan, 1995).

Findings of the Culnan's (1995) study and Szekely's (2010) study in the context of Hungary about young peoples' privacy concerns are contrary to Budak et al.'s (2013)

study findings. While the former studies say younger people are less likely to be concerned about privacy the latter sets forth that older people are less concerned about their privacy. Szekely (2010) explains the younger generation's tolerance for privacy violations with socio-political changes in Hungary. In order to enjoy economic prosperity as part of the new capitalist system the technocratic generation is willing to sacrifice to some extent its privacy and accept limits to individual freedoms. Furthermore McCahill and Finn's (2010) study showed how social positions of class and gender influences children's experiences and responses to surveillance.

2.7 Trust and Confidence in Government

One of the most discussed concepts in the privacy and surveillance literature is trust. Researchers have demonstrated that public trust is important for government decisions and policies (Hetherington & Nugent, 2001). Although there has been a general distrust of the federal government in the US through its history, the level of trust may vary according to certain policy issues (Marmura, 2010). A survey study conducted in 2002 after the 9/11 attacks found that 68% of respondents trusted government to handle national security issues, while 38% of them trusted government to handle social issues (Langer, 2002).

When citizens trust in government institutions and officials they are more likely to support government to solve social problems (Putnam, 2000). According to Tilly (2004) it can be expected that if people trust their governments they are more likely to support draconian laws that increase surveillance. In contrast, distrust leads to citizens' withdrawal of support for state policies, questioning legitimacy, tax evasion, not volunteering for military service etc. Although it can be assumed that trust and confidence in government

may allow willingness to exchange civil liberties for security there is not sufficient empirical research evaluating if trust is actually related to support for national security laws and policies (Nakhaie & Lint, 2013).

Marmura (2010) argues that the GPD survey results for questions 17 (whether national security laws intrusive) and 5 (if there is a right balance between security and privacy) do not necessarily indicate whether revealed levels of public mistrust stem primarily from the fear that the state has implemented a too invasive national security policy and hence government is not committed enough to protecting individual rights. He determines that there are polls conducted by ABC News and the Washington Post that reveal inconsistencies between trust and support for policy. For instance while people express the view that the government engage in unjustified intrusions into personal privacy, on the other hand the majority may approve the warrantless wiretaps of the NSA when investigating terrorism. Thus polls show that citizens become increasingly uneasy about government security practices; however a substantial majority of them still remain willing to tolerate threats to privacy in the name of greater security.

In previous studies trust has been examined as an antecedent to privacy, outcome of privacy, and as a mediating/moderator variable (Smith et al., 2011). Previous studies also used respect to authority as a variable. Using the data from World Values Survey of 1981-1983 Baer, Curtis, Grabb, & Johnston, (1995) found that most of the French Canadians who resided in Quebec were relatively less likely to respect the authorities when comparing Americans and English Canadians. This finding also supports the idea that privacy concerns may vary according to demographic variables and cultures.

Szekely (2010) argues that the finding of the GPD survey about the level of trust in Hungary is in contrast with well-known social phenomena and general public opinion. He implies that in most of the former communist countries, including Hungary, there has been a distrust between the governing and governed. Therefore the reported higher level of trust seems to be inconsistent.

It is shown that firms can build trust and thus mitigate privacy concerns by implantation of fair information practices which is also called procedural justice (Xu, Teo, Tan, & Agarwal, 2010). If individuals perceive that private companies are acting responsibly in terms of their privacy and that they provide sufficient legal regulations to protect their privacy, they show less concern about internet privacy and have greater trust and confidence in the power-holders (Wirtz, Lwin, & Williams, 2007). In similar ways governments can inform their citizens about the necessity and contents of regulations about security, surveillance, and privacy.

2.8 Knowledge of Laws

Citizens' familiarity level of the enacted laws has the potential to influence their attitudes towards them. A survey conducted by the University of Connecticut in August 2005, found that even though 64% of the American respondents said they support the US Patriot Act, only 57% said they are familiar with what it includes, and only 42% could identify its primary intent. The results of the study support the view that the more citizens know about the laws enhancing the prevailing surveillance capacities, the less likely they are to support these. Thus, if they knew what the Act implied, their concerns would increase (Marmura, 2010).

When an individual is informed about organizational privacy practices, this can be seen as having a state of privacy awareness (Malhotra, Kim, & Agarwal, 2004). It is suggested that consumers' privacy concerns increased when consumers become aware that organizations have collected and used their personal data without their consent (Cespedes & Smith, 1993). Culnan's (1995) study indicates that consumers who are unaware of personal information procedures tend to be less concerned about privacy than consumers who are aware of privacy procedures. Further, Dinev and Hart (2006) argue that social awareness is a predictor of privacy concerns. People with high social awareness are aware of privacy policies. Moreover, Zureik and Stalker's (2010) assumption is that experience with and awareness of privacy regulations play an important role in shaping people's attitudes to privacy. Following these arguments it can be concluded that citizens' knowledge of privacy laws and regulations may affect their attitudes.

2.9 Emotional Experience with Terrorism

It can be suggested that any emotional experience with terrorism affects citizens' privacy concerns both directly and via the mediating factor of regulations. Due to terrorist incidents or terrorism threats, governments may adopt aggressive laws violating civil liberties, and this may trigger privacy concerns or inversely, the public may support the government regulations because of the risk of terrorism (Nakhaie & Lint, 2013). A study exploring the effect of Madrid terror attacks on ideological orientations found that the public's conservative values and negative feelings against non-target groups increased, whereas their attachment to liberal values declined at that time (Echebarria-Echabe & Fernandez-Guede, 2006). According to Marmura (2010) citizens support government surveillance when the threat of terrorism and the need for national security is strongly

associated in their mind. The immediacy, novelty, and tangibility of a terrorism threat is related to the voluntary relinquishing of civil liberties and privacy (Kossowska et al., 2011).

2.10 Regime and Democracy Level of the Country

Certain historical, social, and political characteristics of countries may determine their citizens' attitudes. Using the examples of Mexico and Brazil, Botello (2010, in Zureik et al., 2010) indicated that both countries have experienced authoritarian regimes for a long period of time. As well, Zireik et al. (2010) argued that historical factors can play an important role in shaping attitudes toward privacy. This group uses Hungary as an example, a country where privacy was not regarded possible during the time of the oppressive communist rule. When citizens have difficulty in holding state officials accountable for their actions, countries become less democratic. Therefore, the lack of traditional democratic values may reduce people's safety and security (Cockfiled, 2010a). Privacy has been seen as being fundamental to the protection of individual rights and a stable liberal democracy (Schwartz, 1968).

2.11 Cultural Differences

Even though the US and Canada have been viewed to be culturally similar by many authors, Margulis et al. (2010) indicates that they may be similar, but not identical and Canadian data contrasts with the American because of socio-political differences. If the trust is accepted as a cultural value of a nation it can be said that Canada and the US differ in their level of trust of government. In American values there is emphasis on liberty, egalitarianism, individualism, populism, anti-statism, distrust of centralized authority, and laissez faire. In contrast, the Canadian value system, is exemplified by the Loyalist, and includes elitism, particularism, collectivism, and acceptance of authority (Lipset, 1996).

Previous studies indicate that there are differences in information privacy concerns across cultures (Dinev et al. 2005). Conducting cross-cultural surveys renders culture a possible influencing variable, therefore enabling researchers to examine how cultural values shape economic, social and political spheres. Cross-cultural surveys allow the formation of theories which are interdisciplinary and integrate subfields of a discipline (Inglehart & Welzel, 2004). The pioneers of cross-national studies of privacy from the consumer perspectives have been the researchers from business schools. It is hypothesized that cross-national values will be associated with differences in privacy concerns (Bellman, Johnson, Kobrin, & Lohse, 2004). Societal values, as a basic component of culture, provide an introduction to what is considered important (Zureik & Stalker, 2010). Differences in cultural values stem from factors such as history of the country, economy, technology, geography, religiosity, and demographics. Those factors remain relatively stable over time (Hofstede, Hofstede, & Minkow 1991). Hofstede's (2001) cultural values approach has been used in various cross-national empirical research studies including comparisons and correlations between national cultures and privacy concerns. Initially Hofstede developed four main indicators about national cultures. Those include; "Individualism index (IDV)", "Uncertainty Avoidance Index (UAI)", "Power Distance Index (PDI)", and "Masculinity Index (MAS)". Later he developed the Long Term Orientation (LTO) and Indulgence (IND) indicators. Countries scoring high on IDV tend to be more self-reliant and prefer loose communal bonds, therefore more privacy. Those with high UAI scores tend to be low risk takers and those who score high in PDI favor authoritarianism and acceptance of inequality in the country. Again high scores on the UAI and PDI have indicated high privacy concerns in past studies. Higher MAS reflects male centered values in a society

and assertiveness in contrast to caring values. While LTO means attachment to tradition, IND stands for weak control when raised and reflects the extent to which people try to control their desires and impulses (Zureik et al., 2010; Hofstede, 2014).

Milberg, Smith, & Burke (2000) used a formative index to combine four of Hofstede's (1991) cultural values indices, IND, PDI, MAS and UAI, into an overall measure of cultural values. They found a significant and positive effect on information privacy concerns across countries. The regression weights for the four indicators showed that concerns about information privacy were positively associated with PDI, IND, and MAS, and negatively associated with UAI. Later Bellman et al. (2004) used the first four cultural values and classification of laws according to being sectoral, self-regulated, and omnibus in order to measure their relationship with information privacy concern and consequently found some significance.

2.12 Experience with Security/Surveillance Measures

The experience with privacy violations and national security measures can be associated with privacy concerns. For instance Smith, Milberg, & Burke (1996) found that citizens who have been exposed to measures or have been victims of personal information abuses are likely to have stronger privacy and surveillance concerns.

2.13 Personal Characteristics

Still another source of privacy concerns is said to be based on individual personal characteristics. Xu, Dinev, Smith, & Hart (2008) drawing on information boundary theory suggests that privacy concerns form because of personal characteristics or situational cues that allow individual to assess the consequences of information

disclosure. The differences in personal characteristics such as “introversion versus extroversion”, “independent-self versus interdependent-self”, and “big five” personality traits (Bansal, Zahedi, & Gefen, 2010) are found to have relationship with individual privacy concerns (Smith et al., 2011).

2.14 Role of the Technology

One of the aspects of the privacy debate is the role of the technology, because advances in technology have digitally dissolved the walls of privacy. That dissolution is permeated by cultural values and those values characterize the relationship between privacy and surveillance (Botello, 2010). Governments deploy powerful communication, information, and genetic technologies that increase their capacity to collect, use, and share personal information, therefore a broader attention to privacy is required (Cockfield, 2010b). The social value of privacy is described as setting boundaries for the state’s exercise of power. Political scientists, sociologists, and other social scientists have explored how advances in surveillance technology increase the risk of unexpected adverse social consequences (Regan, 1995). Citizens’ experience with technology has also been assessed in terms of its relationship with privacy attitudes and people’s perceptions of the effectiveness of privacy laws (Zureik et al., 2010). It is assumed that technology may affect privacy issues in two ways. While it may lead to new privacy concerns and outcomes at the same time it has the potential to provide privacy protection and privacy enhancing applications (Smith et al., 2011; Cavoukian & El Emam, 2013). It is obvious that Internet technology has completely changed the grounds of any privacy debate, however, this has given the scholars reason to suspect that another technological development might shift the direction of the current understanding of privacy. For instance Cavoukian and El Emam,

(2013) propose, “Privacy Protective Surveillance”, a new type of technology that would be blind to personal information until it found the key elements to suspect that there is a threat and would foster the need to examine personal information. Although technology and regulations should go hand in hand (Garfinkel, 2000), the privacy laws and the court decisions related to these have been slow to catch up with technology (Shipler, 2011).

Relevant with the effect of technology in our lives and the importance of legal regulations Cockfield (2010b) describe the concept of “soft determinism”. According to this approach, technological developments are embedded in our social, political, economic, and other processes and serve to configure future actions and relationships with technologies and their users. It is accepted that technology shapes the present situation and has a determining effect on human affairs; however individuals and groups can still control the harmful aspects of this determinism and the effects of technological developments by setting up legal rules and policies. Another concept “compatibilism” accepts that individuals’ choices and decision making are constrained by everything outside the mind and everything inside the mind, but still people can exert free will if they are not coerced by others. In other words free will and determinism are compatible with each other.

2.15 Surveillance and Privacy Regulations

Individuals in a society are linked to the state with a social contract. That social contract consists of laws that regulate social life by determining both the duties and responsibilities of the state and its citizens (Wraight, 2009). Therefore, states themselves have to comply with the laws authorizing surveillance powers and laws safeguarding individual privacy.

Fura and Klamberg (2012) argue that four major changes in our society have prompted a need to reform both the tools of electronic surveillance and domestic legislation. These changes include: Technology, perception of threats, interpretation of human rights, and ownership of telecommunications. Threats to national security have shifted from military threats to non-state actors such as criminals or terrorists (Hough, 2008). This has led to preventive and further proactive and preemptive regulations and intelligence. However, Webb (2007) indicates that the preemption is extremely dangerous because it justifies almost anything.

Among legislative measures taken after 9/11 in the US, and the most important one, is the USA PATRIOT Act, which is the abbreviation of "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (Ebenger, 2008)". The Patriot Act and the FISA Act are the most highly discussed pieces of legislation in terms of privacy and mass surveillance. With the USA Patriot Act of 2001 and 2006 surveillance capacities were enhanced by programs known as "Bulk Phone Records Program" or "Section 215 Programs". A further provision of the Patriot Act was entered into force in 2006, and allowed the surveillance agencies demanding access to "any tangible things" if presumed related with potential criminal or terrorist activity. This amendment also authorized the NSA to collect phone call records. In 2008 Congress passed Section 702, an amendment to FISA Act. Then, the PRISM Program enabled the NSA to collect data from internet companies, emails, voice calls, videos, photos, chat services and other forms of communication (S. Taylor, 2014).

The Patriot Act was seen as a necessary tool, but was criticized as well. It was criticized for extending surveillance powers of the state dramatically and creating a "Big

Brother" and a "surveillance state". Moreover it was said that it made amendments to the ECPA of 1986 and reduced its protections. Critics argued that the government should not have more power than t needed (Kerr, 2003). However, powers given within the Patriot Act diminished the due process requirements, and allowed for more video surveillance of public spaces; more eavesdropping on conversation; more identity checks; and more scrutiny of daily activities, transactions, purchases, travel, and financial flows. Those who objected to Patriot Act's regulations were easily blamed as being selfish and the statement that privacy is a "selfish" value needs to be sacrificed for the well-being of society and collective benefits of security (Nissenbaum, 2009). After the debates over the NSA's bulk data collection authorities provided by The Patriot Act, the Freedom Act entered in the force in June 2015 and replaced the Patriot Act and reduced the investigative power of the NSA (Diamond, 2015).

The debate on privacy and security always touches on the Fourth Amendment of the US Constitution (S. Taylor, 2014). The constitutional protection of privacy is not absolute and the Fourth Amendment does not altogether deny the government access to the information which is necessary to perform its duty to secure the land. Rather, it seeks to minimize or avoid the dangers inherent in surveillance by restricting the techniques and methods that the government may employ to collect that information (Fiss, 2012). Even though the word privacy is never mentioned in the US Constitution, liberal and moderate judges imply the term privacy is woven into the First Amendment's rights of worship, speak, and assemble and into the Fourth Amendment's protection of "persons, houses, papers, and effects against unreasonable searches and seizures" (Shipler, 2011).

The U.S. Supreme Court has a legislative role in the US. With the advances in technology and social change it was seen that the decisions of the Supreme Court about the frame of the fourth amendment's privacy protections had changed over time. In this vein, in 1928 Olmstead case (Olmstead v. United States) the Supreme Court ruled that an unauthorized wiretap did not violate the constitutional right stated in the Fourth Amendment. However, later in 1967 the court reversed the decision ruling that a person had reasonable expectation of privacy when talking in a public phone booth (PoKempner, 2014). In 1979, with the development of the analog-era of the technology, in the Smith v. Maryland case the Supreme Court this time ruled that government can collect the phone numbers called over a short period and allowed the NSA to store this data for five years in a massive database. The reason for allowance was that individuals had no reasonable expectation of privacy concerning the phone numbers they called. This was because of the fact that a person already share that information with phone companies for billing purposes when making phone calls. When the third party has access to personal information government assumes that this information is public and not under the protection of Fourth Amendment.

The discussions on surveillance and privacy laws continues to unfold around the adequacy of laws or whether reform is needed, whether the current surveillance practices are lawful or whether the legal limits exceeded, and if there are certain gaps that need to be regulated (S.Taylor, 2014). Even though national security and surveillance regulations are considered lawful by citizens, they can be seen as intrusive upon the individual rights and civil liberties (Zuriek et al. 2010). Most scrutinized countries in terms of mass surveillance are the US and the UK with their higher technological capacity agencies the

NSA and GCHQ (Privacy International, 2014). The restriction of civil rights by introducing national security laws in state of emergency might be acceptable to some extent until the threat is eliminated; however these laws are seldom reverted to in the normalcy of peacetime and remain in force (N. Taylor, 2014).

Mainly two views have been voiced on the adequacy of privacy and surveillance laws in the US context. The first view was that the laws currently in force was inadequate to maintain the balance between national security and individual privacy and there was a need for revisions of Fourth Amendment and other privacy laws (Cole, 2014). On the contrary Garfinkel (2000, p.119) says: "What needed are not new laws, but a commitment to enforce the many laws that are already on the books." The protection of both security and privacy are regulated with these laws.

Banisar and Davies (1999) introduced four models for privacy protection. These included "comprehensive laws, sectoral laws, self-regulation, and technologies of privacy". Most of the countries adopting data protection law prefer the "comprehensive laws" model. This model is encouraged by the EU for purposes of ensuring compliance with its data protection regime. The enforcement of the rules is overseen by an official or agency. This official can be a commissioner, ombudsman or registrar.

The US and some other countries refrain from general data protection rules in favor of specific "sectoral laws". A major weakness of this approach is that protections frequently fall behind because they require that some form of new legislation is introduced with each new technology. In this system the lack of an oversight mechanism is seen as a problem.

The “Self-regulation model” is about the private sector’s own privacy regulations. Theoretically, data protection can also be achieved through self-regulation. For instance, private companies can establish codes of practice to protect the privacy of their employees and customers.

The last model “technologies of privacy” refers to individual attempts to protection of privacy by benefitting from available technology. With the development of commercially available technological systems privacy protection can be achieved by individual users. These individual technology based protections include encryption, anonymous remailers, proxy servers, digital cash and smart cards (Banisar and Davies, 1999).

Bellman et al. (2004) has used Hofstede’s cultural values and the classification of laws according to being sectoral, self-regulated, and comprehensive. Their research in business literature includes the investigation of the relationship between the privacy concerns of consumers and the type of laws according to above classification. They hypothesize that consumers from countries with a comprehensive privacy regulatory structure will have higher levels of privacy concerns compared to consumers from countries with sectoral privacy regulation or no privacy regulation. They found that consumers in countries with sectoral regulation have less desire for more privacy regulations.

Milberg et al. (2000) suggest that if consumers do not perceive firms as adequately protecting their privacy, they will distrust self-regulation as a process and prefer state intervention, which can eventually lead to a regulatory response. For instance, in the United

States, there are sector-specific laws for specific types of records such as credit reports and video rental records and for classes of sensitive information such as health information (Smith, 2004). In thinking of a similar relationship between citizens and the government, it can be said that when citizens do not perceive privacy laws that are already in effect as adequately protecting their privacy, they will find the laws intrusive or inadequate and will demand better ones.

It can be argued that the European laws on privacy and national security surveillance do not diverge significantly from the US law. The ECHR permits bulk surveillance of communications of foreign nationals abroad based on very substantial criteria mainly including threats to national security and the economy, and threats of serious crimes. In a democratic society government is expected to be transparent in its acts, however, the ECHR has understood that a more detailed specification of conduct could enable possible wrongdoers to adopt new behaviors to avoid surveillance (Margulies, 2014). The general comparisons in terms of privacy laws between the US and the EU take into account the Fourth Amendment of the US Constitution and the 8th Article of the ECHR (Fura & Klamberg, 2012).

The EU's Directive on Data Protection (1995) urged nation states to adopt privacy laws for purposes of personal data protection including data protection authority (Ybarra, 2011). If we compare the US and the EU in this respect, it can be said that the US denies citizens expectation for privacy of personal information, which is already available to the public. The US law presumes that people lose their privacy interests in particular ways once they voluntarily disclose certain pieces of information in any public setting. But, in the EU, personal data is defined to cover any information related to an identified or

identifiable person. Europe treats privacy as a human right, rather than just an economic good (Shane et. al 2004). In Europe, the privacy law has developed as a form of ensuring personal dignity, in contrast to the US, which is developed on the basis of the liberty concept. Hence, it is concluded that the EU has taken on a more regulatory role in the realm of informational privacy than the US. Ybarra (2011) also argues that the UK possesses the least stringent data collection laws in Europe, while the strongest privacy law has continued to be that articulated by Germany.

Previously, the EU Data Retention Directive had obligated Communication Service Providers (CSP) to collect and store citizens' communication traffic data. However, in 2014, the Data Retention Directive allowing CSPs to retain the traffic data for two years period was abolished because of privacy concerns (European Court of Justice [ECJ], 2014).

The Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) are the key instruments for ensuring fundamental human rights are in place across the globe. Beside the prevailing national laws, Article 12 of the Declaration and Article 17 of the ICCPR regulates the protection of the right to privacy. All the countries of interest in the study except China have already acceded or ratified the ICCPR and these along with their provisions are legally binding. China has signed, but has not ratified the covenant yet, as of May, 2016. Further, the UDHR was not originally intended to be a binding force when it was first opened for signature to participating countries in 1948, however its provisions have since gained an almost binding like character as far as being the most customary law (Office of the United Nations High Commissioner Human Rights, [OHCHR] 2015).

Table 2.8. ICCPR's Signature, Accession and Ratification Status of Eight Countries

Countries	*Signed*	*Ratified (R)/Acceded (A)*
US	5 Oct 1977	8 Jun 1992 (R)
Canada		19 May 1976 (A)
Brazil		24 Jan 1992 (A)
France		21 Jan 1983 (A)
Spain	28 Sep 1976	27 Apr 1977 (R)
Hungary	25 Mar 1969	17 Jan 1974 (R)
Japan	30 May 1978	21 Jun 1979 (R)
China	5 Oct 1998	*Not ratified

Source: http://treaties.un.org

Margulies (2014) discusses the jurisdiction aspect of the privacy protection laws with reference to the Fourth Amendment, the ICCPR Article 2(1) and Article 17. The Fourth Amendment is generally interpreted to provide protection only for US citizens or legal permanent residents or those physically present in the United States. Surveillance of non-US persons abroad is not seen as problematic under the domestic law. However, there is an opposite view that the US has obligations under international law to respect the privacy of persons even if they are not present in their homeland (PoKempner, 2014). This view is based on Article 17 of the ICCPR, which protects individuals from "arbitrary or unlawful interference with privacy home or correspondence" and Article 2(1) that implies each state party must "respect and ensure to all individuals within its territory and subject to its jurisdiction." The author proposes a middle way called "procedural pluralism" which means "flexibility in the procedural safeguards the state chooses, as long as those safeguards provide meaningful constrains on government. This model gives states flexibility adopting core principles for protection such as notice, oversight, and minimization (Margulies, 2014, pp. 1-3)."

Researchers regard regulations and legislation among the best methods of privacy protection (Garfinkel, 2000). Countries with authoritarian regimes generally are accused

of being surveillance states. Nevertheless, it is indicated that no matter how mature a democracy is, the risk of surveillance practices being non-democratic, is real. Even though there is a legal framework to regulate surveillance technologies in democratic states it does not necessarily prevent the spread of mass surveillance. With the development of surveillance technologies the pervasive use of surveillance for deterring and preventing crime and terrorism may continue to be used despite the existence of regulatory frameworks. This is the main concern of the privacy advocates (Privacy International, 2014).

The problem of privacy includes the need for, the use of, and the storage of personal information. Governments are supposed to protect its citizens from threats both inside and outside the nation-state. Therefore, a certain amount of personal information is necessary. The controversy is on how much is necessary and how best to safeguard such sensitive information. This varies with time and culture (Martin & Rabina, 2009). The data retention is a sub-topic of privacy regulations. To reduce the risk of privacy violation the proposed suggestions are; the adaption of minimal data retention policies, the building of strong encryption into products, and directing legal teams to fight claims on behalf of users (Soghoian, 2012). Since activities conducted in the name of national security often went far beyond the required and lawful scope, there is an apparent need for accountability and control over the intelligence community. De Rosa (2003) points out two types of privacy protection. One of them involves restrictions and prohibitions and the other, oversight and control. In contrast, the absence of healthy oversight may result in a lack of confidence in the government (De Rosa, 2003).

De Rosa (2003) also argues that it is possible to adapt to new needs without undermining civil liberties or privacy. As a policy implication the author suggests less prohibition of the processes of collection and dissemination of private information, but more effective oversight and control over government activity. Further, clear guidelines that must include guidelines about relevance, dissemination, retention, and reliability, training and integrative oversight can be adopted. Public involvement, open discussions, and executive branch's openness with congress are additional suggestions. As well, technology can be used to protect privacy such as special access requirements, and reliable methods for user authentication. Hence, it seems that the author is more in favor of the use of oversight and control than restrictions and prohibition. In contrast, Cavoukian (2014) asserts that limits on the collection of personal data should be central to the protection of privacy. Basically, if governments do not collect large amounts of data, they cannot abuse or lose control of this process. This author emphasizes that once the harm has been done it is difficult to correct this. In this digital age the majority of privacy breaches and data leaks remain unknown, unchallenged or unregulated.

A specific mode of control is that carried out by the FISA Court system in the US. However, it is criticized for not giving careful scrutiny to warrant applications and it approves almost every application. Only a very low percentage are denied. Moreover, it is criticized because it hears the story only from the governmental aspect. For a solution of this problem, a publicly understood and trusted oversight mechanism is suggested. A panel of public advocates who would represent privacy interest before the FISA Court is a further option for solution (S. Taylor, 2014; Rule, 2007). On the other hand, Margulies (2014) proposes that an institutional public advocate to counter government arguments in court

would enhance the legitimacy of US surveillance even more than a panel of lawyers. Still another proposal by Garfinkel (2000) suggests the creation of a permanent federal oversight agency charged with protecting privacy. This agency would perform reviews of new federal programs that have the potential for privacy violations before they are launched. It would enforce existing privacy laws and perform duties similar to those of an ombudsman.

The privacy advocacy organization "Privacy International" has evaluated national laws regarding privacy and surveillance and calculated privacy index scores according to fourteen specific criteria. As such, index scores countries have been categorized to examine if they have endemic surveillance problems or they protect human rights (Privacy International, 2014; Zureik et al., 2010). More information about Privacy International's evaluation of the countries is included in the methodology chapter. Privacy scores however, give one an idea about the stance of privacy protections ensured by privacy regulations in a given country and can be used after that as suggested by Zureik et al. (2010).

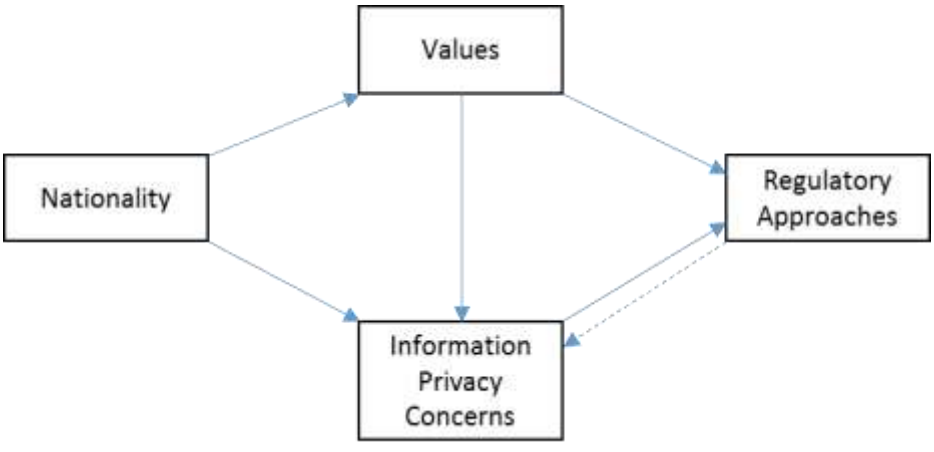
2.16 Empirical Research on Privacy Concerns

Information technology developments together with the increasing value of information to policy-makers have caused rising concerns about information privacy management. Milberg et al.'s (1995) study examined the relationships among nationalities, cultural values, and personal information privacy and personal information regulations in the context of business operations in nine countries (Australia, Canada, Denmark, France, Japan, New Zealand, Thailand, the UK, and the US). Their study taken from the business literature was one of the first cross-cultural and empirical studies investigating information

privacy concerns. The information privacy regulation models of these countries were categorized as: self-help, the voluntary control model, the data commissioner model, the registration model, and the licensing model. They used Hofstede's three cultural dimensions to investigate the associations both with information privacy concerns and regulations. The study found that personal information privacy concerns vary across countries. The cultural dimensions of PDI and UAI were found to have a significant relationship, and the IDV had a significant negative relationship with information privacy regulations. Countries with either "no privacy regulation" or those with the strictest model of privacy regulation, "registration model", were significantly associated with lower information privacy concerns than those using the other three models. Thus, countries with more moderate regulatory structures were associated with higher aggregate levels of concern, and those levels of concern were not significantly different from one another.

The privacy concern model developed by Milberg et al. (1995) was later modified by Zureik et al.'s (2010) study and was further benefited by this current study.

Table 2.9. Proposed Model for Studying Information Privacy Concerns



Source: Milberg et al. (1995)

Milberg et al. (2000) in their later study argued that most of the developed countries had issues with the trade-offs between access to information which enabled economic efficiency and individual right to privacy. Their study included examinations of the associations between cultural values and information privacy concerns, between cultural values and regulations, and between information privacy concerns and regulations. Different form their earlier study of 1995 they covered 25 nationalities from 19 countries by using the Information Systems Audit and Control Association's (ISACA) 595 usable surveys from internal auditors of its 63 chapters. The regulations referred to government involvement in corporate management in the study and were handled under five categories. They found that country's regulatory approach to the corporate management of information privacy was affected both by cultural values and individual's information privacy concerns. Hofstede's cultural values of IDV, PDI, and MAS were each found to have a positive effect on the overall level of information privacy concerns, whereas the UAI value dimension had a negative relationship with the level of privacy concerns.

Margulis et al. (2010) compared personal information concerns of the US and Canadian respondents by using GPD survey data. They examined the associations between the responses related to citizens' privacy concerns and the responses about citizens' self-reported knowledge of privacy laws and belief in their effectiveness. In addition to knowledge of laws they looked to the same relationships with citizen's reactions of not giving or giving false information to organizations, the appropriateness of ID cards, and employers' personal information sharing with third parties. Self-reported knowledge of privacy laws, the belief in the effectiveness of these laws, behavioral reaction responses, views about ID cards, and thoughts about government and private sector information

sharing were used as dependent variables in their study, while privacy concern related questions consistent with the Harris-Westin index were considered to be independent variables.

Findings of their (2010) research demonstrated that citizens' belief in the level of their own "control over personal information" had a significant relationship with "knowledge of laws" about government protection of personal information, both in the US and Canada. Only for Canada, where the low level of trust of government was observed to be about striking the right balance between national security and individual rights, was a positive relationship with level of knowledge about laws found. A significant negative relationship was found between the appropriateness of private companies' information sharing with other companies and knowledge of laws about government protection of private information for the US. Both for Canadian and for US respondents there was a significant relationship between high level of trust in the right balance and the belief that personal information protection laws were effective. Only for Canadians was a positive relationship found between the perceived effectiveness of privacy laws and the belief in one's ability to control personal information. In addition, the approval of national ID cards was found to be associated with the belief that the government would be effective in protecting the information from disclosure in both countries. Canadian respondents who support national ID cards believed that they had less control over personal information than other countries. For both countries the view that government agencies should not share personal information with other government agencies and private companies was associated with the view that private companies should not share information with government organizations and other private companies.

Margulis et al. (2010) found little evidence to support the relationship between attitudes and behavior as a reaction even though they asserted that the US respondents were more likely to take action. As a result, they found significant differences between cultures in the structure of privacy concerns. Canada and the US provided five different privacy concern factors that one crossed national borders and four did not. This strengthened the proposition that privacy concerns are culturally specific.

Based on the GPD survey and that taken by seven countries Grenville (2010) investigated citizens' reactions to surveillance practices in order to protect their own personal information. Grenville developed a model to examine why some of the respondents resist, while others accept or ignore the issue. The dependent variables in the study were the actions taken to protect personal information. The resistance to surveillance was operationalized as refusal, discovery/counter-surveillance, blocking, and avoidance actions. The independent variables of the study were knowledge of surveillance technology, awareness of being monitored and detention at the airport, trust in government about the right balance between national security and privacy, and control over personal information. The author used a statistical analysis to identify and define the segments of respondents as status quo satisfied, informed resisters, and alienated skeptics. The study found that Canadians and Americans were the most resistant to surveillance while Brazilians and Mexicans were the least.

Fournier (2010) examined the national sub-groups of Quebec and the Rest of the Canada (ROC) again by using the GPD survey. In the first section of this study, the author was interested in the comparative perceptions of individual control, knowledge of laws, and degree of proactivity regarding personal information. In the second section the

comparative perceptions of trust about ID cards and database, and information sharing with third parties in public and private sector were examined. Fournier found that the ROC respondents were more aware of laws, and that they felt they had some, a lot or a complete say over personal information, they took action to protect personal information within private sector, and they were worried about providing personal information on websites. On the other hand more Quebecers somewhat agreed and strongly agreed with the ID cards (the belief that government can protect personal information exists in the ID cards) and were supportive of information sharing. The author concluded that even if there were some differences between the two sub-groups this was not a sign of a significant culture gap, instead more than half of the survey questions investigated in the study showed that they were in tune. ROC and Quebec respondents displayed more faith in government and public agencies than in the private sector and the majority from both groups agreed to information sharing depending on conditions.

Still Nakhaie and Lint (2013) used the GPD survey to investigate citizens' support of government surveillance policies. They studied citizens' attitudes toward surveillance and security-based legislation by placing the notion of "support" instead of "concern" in the center of their study. Their units of analysis were the two sub-regions of the US and Canada, which they believed were different sub-cultures. These regions included the South US and the rest of the US, Quebec and the Rest of Canada. Responses to four questions from the GPD survey were taken together as a dependent variable indicating the citizen's support for security and surveillance policies. These four questions were about government information sharing, private companies' information sharing, views regarding national ID's, and travelers' information control. The researchers regarded the respondents'

statements of trust in government to have about the right balance, airport officials' respected privacy, and low tolerance for minorities and demographics such as education, age, gender, and province served as independent variables. They found that a lower level of tolerance for minorities, the perception that airport officials can protect private information of travelers, and trust in government about striking the right balance between national security and individual rights were all strongly and significantly related to citizens' support of prevailing security and surveillance legislation.

The research conducted by Zureik (2010) on seven cities in China highlighted the correlates of internet use and public attitudes towards various surveillance technologies and privacy issues. Zureik used data from both the GDP survey and China Internet Network Information Center's (CNNIC) survey for his study. The relationship among the familiarity of the various surveillance technologies, experience in using the internet, the privacy laws governing the use of these technologies in the private and public sectors, and the efficacy of the laws were explored. The national data showed that internet usage in China increased in the last decade. The lower income people and people having semi-skilled and unskilled occupations were the underrepresented groups among the internet users. Overall, region was not a predictor of internet usage in seven cities of China. Citizens' knowledge about technology was higher than their knowledge of privacy laws in both private and public sectors. A positive relationship was found between the two. In addition, the perception of privacy laws' efficacy was not found to be significantly associated with either knowledge about technology or knowledge about privacy laws.

Bellman et al. (2004) investigated the predictors of internet (online) privacy concerns revealed by national regulations. The differences among internet privacy

concerns were attributed to cultural values, internet experience, and desires of political institutions. The authors conducted their own survey with e-mail invitations reaching 534 respondents. They used Hofstede's four indices as cultural value dimensions and regulations and the Privacy International's 1998 classification of country's privacy regulations as; omnibus, sectoral, and no regulation (self-help). The demographic variables were taken as control variables. Using a sample of internet users from 38 countries they found support for the variables of cultural values and internet experience being associated with internet privacy concerns. When internet experience was high, privacy concerns were low. Controlling for internet experience, cultural values were significantly associated with privacy concerns. The regulatory differences mediated these cultural differences. However, when differences in regulation were harmonized, new cultural values emerged. It was found that three of the Hofstede indices (PDI, IDV, and MAS) had an impact on privacy concerns in the opposite direction to that previously reported by Milberg et al. (2000). They concluded that consumers in countries with sectoral regulation had less of a demand for additional privacy regulations.

Dinev and Hart (2004) considered one of the definitions of privacy and investigated two themes included in the definition affect privacy concerns. The definition they were interested in was whether "Privacy represents the control of transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or minimize vulnerability (Margulis, 1977, as cited in Dinev et al. 2004, p. 414)." Therefore they explored the effects of the independent variables; perceived control of personal information and perceived vulnerability to the information privacy concerns. They conducted a survey by taking a sample of 365 individuals in the Southeast region of the US including

undergraduate and graduate students, employees of public schools, two high-tech companies, a banking institution, a small number of retail and service businesses and others reached by direct mailing in a neighborhood. They found support for perceived vulnerability variable, but moderate support for the perceived control variable over personal information.

Based on the literature and with the guidance of the previously mentioned studies, this present study developed its own model with the variables both included and not included in the previous research. These variables are described in the methodology chapter. However, not only are the independent variables of the study triggered to focus on the topic of privacy concerns, but specific events such as whistleblower's leaks and other revelations about the intelligence communities' surveillance capacities and practices are discussed. Good examples here are the Watergate Scandal and former NSA contractor Edward Snowden's revelations on the NSA surveillance (Poitras, 2015). The PEW's public opinion polls about privacy and security shows significant differences before the leaks and after the leaks (PEW, 2013).

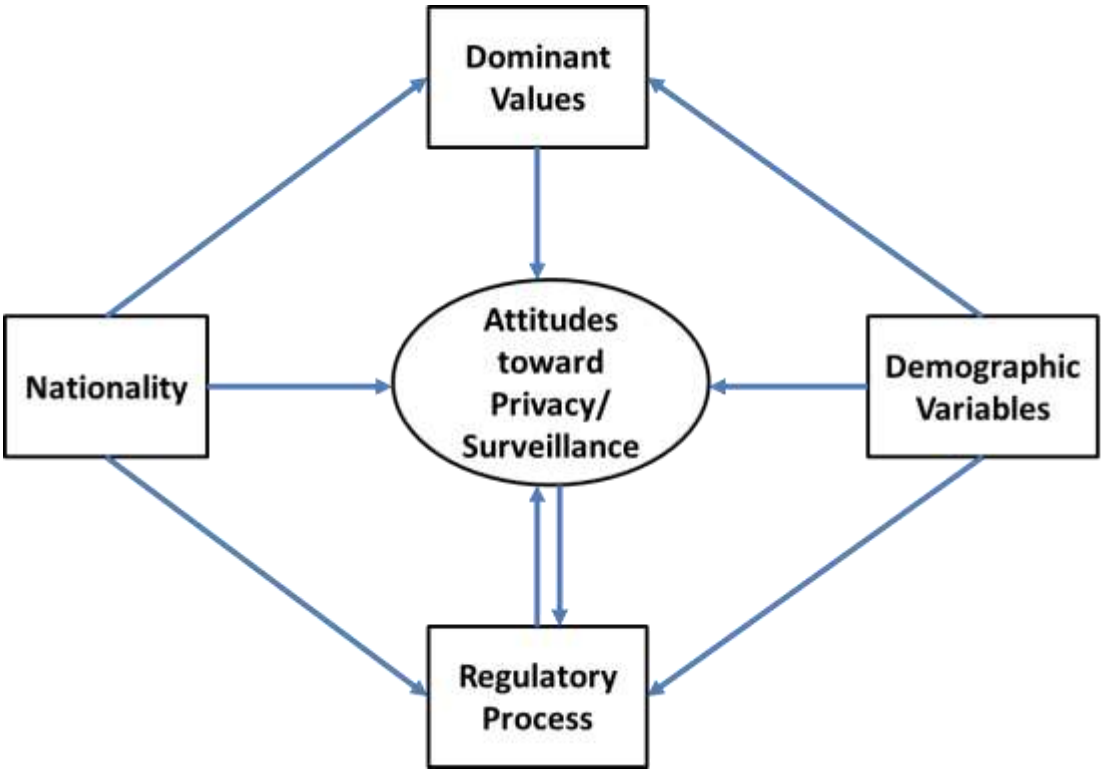
Wirtz et al. (2007) indicates that additional attitudinal studies about privacy, data protection, surveillance, and security can help to understand individuals' behaviors, and those behaviors would require different policies.

2.17 Privacy Concern Models

Drawing on Milberg et al.'s (1995) study, Zureik et al. (2010) modified their proposed model by adding demographic variables and making it more compatible for

studying privacy attitudes toward state policies, rather than corporate policies. Their model is shown below:

Table 2.10. Surveillance and Privacy Attitudes Model

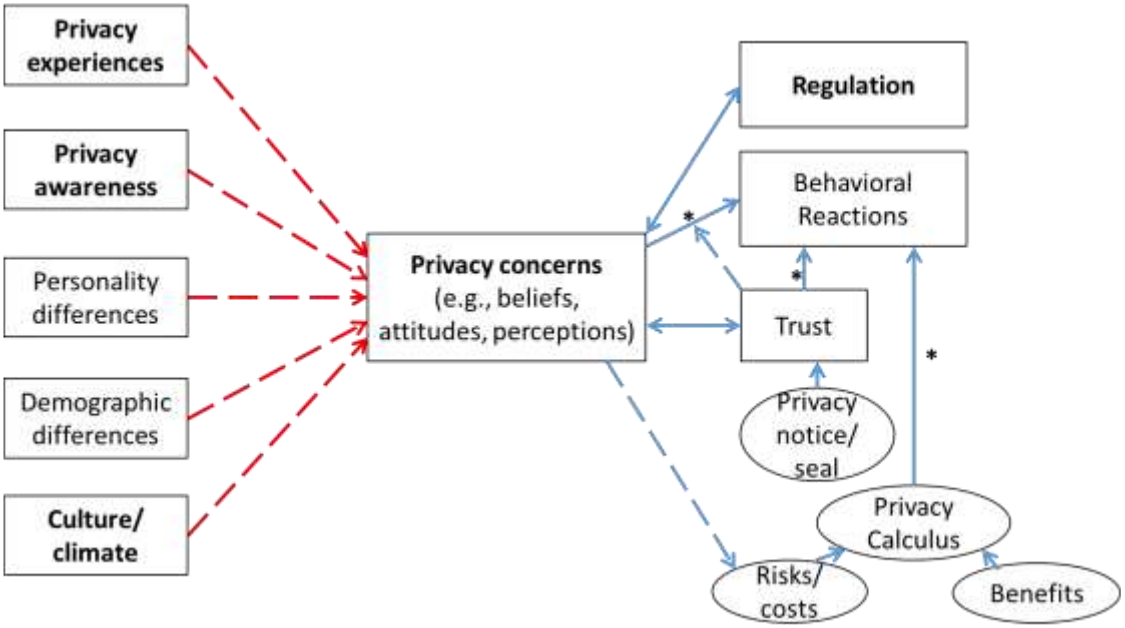


Source: Adopted from Milberg at al.'s (1995) study and further modified by Zureik et al. (2010).

Empirical studies about privacy from different disciplines have examined the relationship between privacy and other constructs. Reviewing prior studies and considering an optimal way to study privacy attitudes Smith et al. (2011) developed the APCO Macro model. In the center of the model they placed the "privacy concern", then the antecedents of the privacy concerns were placed on the left, and outcomes of privacy concerns on the right. They formalized this model as: "Antecedents →Privacy Concerns → Outcomes (APCO)". Privacy concern have been measured at an individual level of analysis. As seen in the model this factor has been studied both as a dependent and independent variable. It

is concluded that the dotted lines between antecedents and privacy concerns represent tenuous relationship, but this has not been confirmed through repeated studies.

Table 2.11. APCO Macro Model: Relationships between Privacy and other Constructs

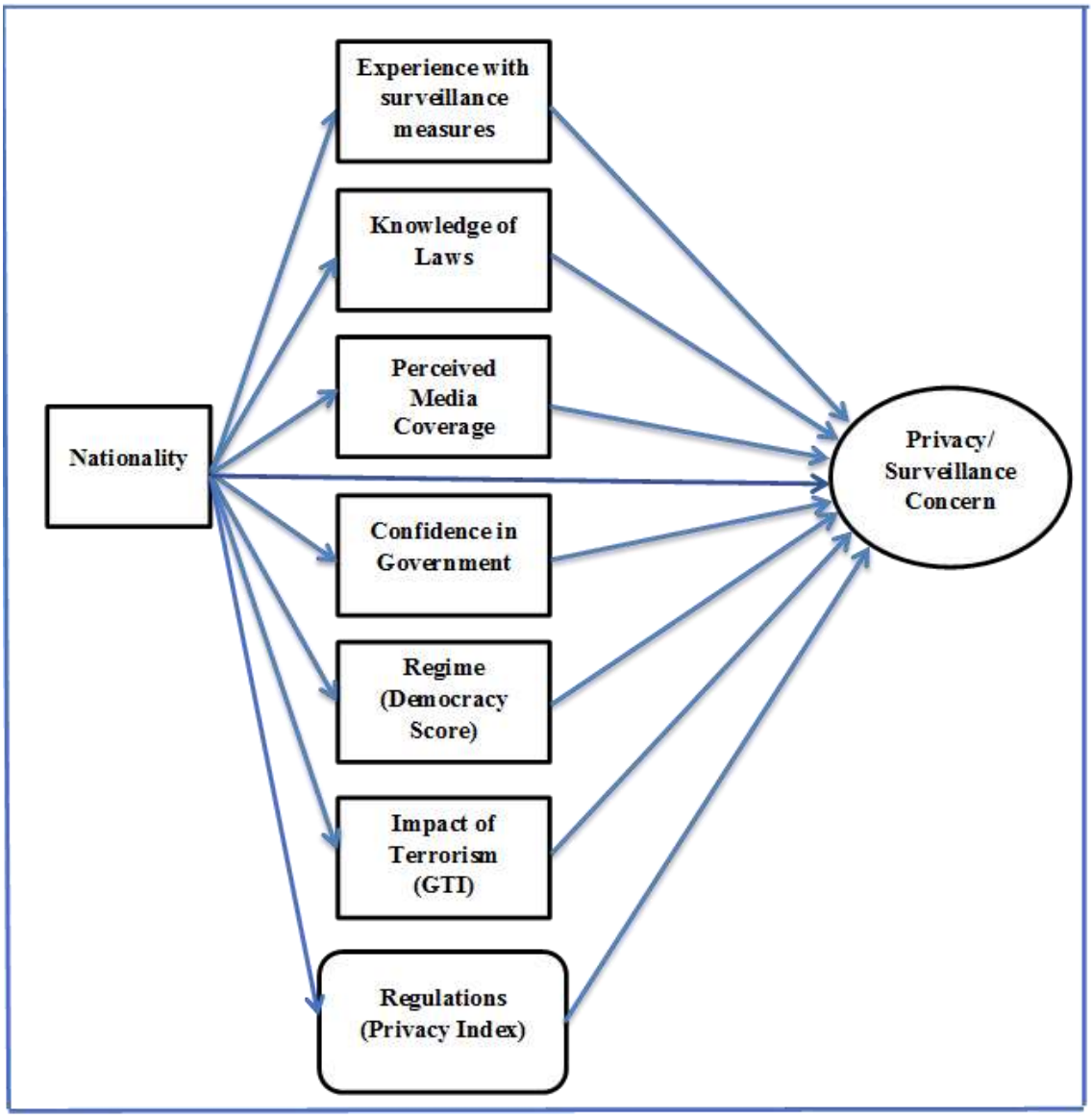


Source: Smith et al. (2011). Information Privacy Research: An Interdisciplinary Review.
(*Indicates that results threatened by privacy paradox.)

Therefore, the current study was interested in examining the determined tenuous relationship on the left hand side of the model and becoming one of the studies that could confirm the relationship between the depicted antecedents and privacy concerns. Even though the interest was on examining the left side of the model or the regulation variable, which has a two way relationship, this was considered as both an antecedent and outcome variable. For instance, if a country had experienced terrorism, this may have led to strict surveillance and security regulations. Then citizens' privacy concerns may increase. If government considered those public preferences and concerns and responded accordingly by softening security regulations as is the case in the "thermostatic model" then privacy

concerns may decline. Therefore, it was assumed regulations can take on the different roles of being an independent, mediator, and dependent variable. The GPD Data, the privacy literature, and the above aforementioned models constituted a base for the development of this model as applied in the present study. This model is depicted below in the Table 2.12. It is further described and analyzed in the next chapter.

Table 2.12. Model: The Antecedents of Privacy/Surveillance Concerns



CHAPTER III

METHODOLOGY

3.1 Research Questions

The current research project was interested in examining the factors that influence privacy concerns, and the relationship between privacy concerns and the related regulations of different nations. To understand this relationship between the antecedents of privacy concerns, privacy concern itself, and the scope of regulations, the current study tried to answer the following questions:

1- What are the correlates of privacy concerns?

2- Do the factors that affect privacy concerns, citizens' privacy concerns, and regulations vary across 8 countries?

3-If they vary, how do they vary across countries?

3.2 Hypotheses

According to the model developed for the study, ten testable hypotheses were examined as follows.

H_1: Citizens' knowledge of law is associated with privacy concerns.

H_1-a. The more citizens are knowledgeable about laws regulating government the more their privacy concerns.

H_1-b.The more citizens are knowledgeable about laws in private sector the more their privacy concerns.

H_2: The exposure to media coverage is associated with citizens' privacy concerns.

H_2-a. The more reported media coverage about protection of personal information the more privacy concern.

H_2-b. There would be a difference between the groups reporting there is more media coverage on terrorism, more violation of privacy by government, and equal media attention to both. If media pays more attention to terrorism there will be less privacy concern, however, if media pays more attention to government privacy violations there will be more privacy concern. If media pays more attention to both, privacy concerns will be moderate.

H_3: Citizens' experience with surveillance measures is associated with their privacy concerns. Citizens who have prior experience with surveillance measures are more likely to have higher privacy concerns than those who are not experienced such measures.

H_3-a. If a person has experienced detention resulting from a search at a border checkpoint he/she will be more concerned about privacy.

H_3-b. If a person has experienced detention resulting in them not being able to board an airplane, he/she will be more concerned about privacy.

H_3-c. If a person experienced detention resulting in being denied entry into a country he/she will be more concerned about privacy.

H_3-d. If a person's personal information has been monitored by a government agency in the past, he/she will be more concerned about privacy.

H_4: The dominant cultural values in a country are associated with citizens' privacy concerns. As a dominant cultural value the more confidence in government in a country the less privacy concerns will exist.

H_5: The impact of terrorism is associated with citizens' privacy concerns. A higher emotional experience with terrorism is negatively associated with privacy concerns.

H_6: The democracy level of a country is associated with privacy concerns. The higher the democracy score of a country the lower will be the citizens' privacy concerns.

H_7: The privacy regulations in a country are associated with privacy concerns. The better the privacy regulations the fewer the number of privacy concerns.

H_8: The privacy regulations vary across 8 countries.

H_9: The privacy concerns vary across 8 countries.

H_{10}: The correlates of privacy concerns vary across 8 countries.

3.3 Data

This study depended on secondary data sets from five different data sources. Among the data sets used in the study, two of them (GPD and WVS) were survey data. Those surveys measured public opinion at the individual level in different countries.

The main data source and the backbone of the entire data set was a survey conducted in nine countries by a Canadian based independent global research company Ipsos Reid as the Globalization of Personal Data (GPD) Project of Queen University's Surveillance Studies Center. The survey data of the GPD project is the most comprehensive and cross-national data available on privacy, surveillance, and personal data protection

issues, which is not only about the corporate private sector. The GPD is an international, multi-disciplinary and collaborative research effort drawing mainly on the social sciences, but also including information, computing, technology studies and law. The project was interested in ethics, politics and policy development around personal data. It investigated why surveillance occurs, how it operates, and what this means for people's everyday lives. This survey is unique because for the first time the same measuring instrument was used across nine countries about citizen attitudes toward privacy and surveillance. The data was obtained from the Surveillance Studies Centre's web site of Queen's University (Ipsos Reid, 2006). The survey was conducted in 2006. The nine countries consisted of: Canada, US, France, Spain, Hungary, Mexico, Brazil, China, and Japan. As a result of the survey, three separate data files were produced. A China file, a Japan file and the remaining seven countries all together in one file.

The GPD Survey questionnaire includes forty-eight questions that measure citizens' knowledge and awareness about technology and laws, the perceived level of control over personal information, trust in government and private companies, experience with measures, citizen reactions to protect personal information, perceptions about media coverage, internet, ID cards, CCTV, information sharing, terrorism and security. It also includes questions about demographics, vignettes, and categories of travelers, workers and consumers (The Surveillance Project International Survey Findings, 2008; Ipsos Reid, 2006). Most of the possible responses to the questionnaire were designed in four choices format using a Likert scale, which is an ordinal level of measurement. In addition, some of the questions included yes/no responses and three choices format. Citizens' attitudes were measured at the individual level.

The second data source was the World Values Survey's (WVS, 2009) Fifth Wave which was conducted over the period 2005-2009. That was the survey employed before the last wave of surveys. This survey has been used in more than fifty countries and is repeated with similar questions about every five years. The data about eight countries of interest were obtained from the fifth wave of the WVS in which the source and data collection years were as follows: Canada-2005, Japan-2005, USA-2006, Brazil-2006, France-2006, Spain-2007, China-2007, and Hungary-2009.

The data source determining the regime type was the Economist Intelligence Unit's democracy index. According to the variable of democracy ratings, countries are categorized as full democracies, flawed democracies, hybrid regimes, and authoritarian regimes. The ratings are listed on a 0 to 10 point scale, and based on sixty indicators grouped in five categories including electoral process and pluralism, civil liberties, the functioning of government, political participation, and political culture. The overall democracy index is the average of five category scores and the category scores are based on the sum of the indicator scores in the category. The country democracy scores were obtained from the data source for the year 2006 (Kekic, 2007).

In order to measure the impact of terrorism, a Global Terrorism Index (GTI) for the year 2006 was used as the fifth data source, and was provided by the Vision of Humanity, the initiative of the Institute for Economics and Peace (IEP, 2006).

The last data source was the international advocacy organization Privacy International survey, which provided the "Privacy Index" scores for the countries of interest.

3.4 Unit of Analysis

The unit of analysis in the present study was comprised of the citizens in 8 countries (Canada, US, France, Spain, Hungary, Brazil, Japan, and China). There are similar studies (Zuriek et al., 2010) considering citizens living in specific geographical regions within Canada and the US as units of analysis. However the units of analysis in this study represent individuals in eight of the nine countries included in the GDP Project.

The countries of interest were selected by the principal investigators of the GPD Project. Those countries can be grouped according to their geographic locations, regime type, and development statutes. The group of countries included in the survey can be considered as appropriate samples for purposes of examining cross-national variations in privacy concerns and its antecedents (Ipsos Reid, 2006). The GPD and WVS survey data used nationally were chosen using a representative sampling method. Further, the quota sampling method was used in the WVS, and respondents were categorized according to gender, age, profession, region, and size of the town. The total sample size of the GPD survey was 9.606 respondents from nine countries. This study investigated eight of those nine countries with a sample size of 8526.

Table 3.1. Sample Sizes and Data Collection Dates of the Countries Included in the GPD Project

	Country	Sample Size	Data Collection
1	Canada	1,001	June 26-July 21, 2006
2	U.S.A	1,000	June 27-July 28, 2006
3	France	1,002	June 27-July 8, 2006
4	Spain	1,000	June 30-July 11, 2006
5	Hungary	1,005	June 27-July 9, 2006
6	Brazil	1,000	July 4-July 7, 2006
7	China	2,002	Aug 5-Oct 12, 2006
8	Japan	516	Dec 21-Dec 23, 2007

Source: (Ipsos Reid, 2006)

3.5 Measures and Variables

3.5.1 Data Merging Process

The original GPD data set consists of three separate data files. The final data set was created by combining those three separate data files. The same survey asking the same questions was conducted in eight different countries. One data set was about the responses to the survey in the US, Canada, Brazil, France, Hungary, Spain. Another data set included the same survey conducted in Japan. The last data set was the same survey conducted in China. During the data merging process, an analysis showed that all the three data sets included exactly the same survey questions, but the coding of the answers was different. To overcome this problem, first the data sets were merged and then recoded in a way that same questions in different countries would have same coding. The coding strategy was

based on the order of the answers given to the questions asked in the GPD survey and included in Zureik et al.'s (2010) book.

In the next step I dealt with missing data in the data set that included all responses to the survey from all eight countries. One strategy concerning missing values in the relevant literature is to use mean value of the non-missing cases across the same survey item (Little, 1988). Therefore, further recoding was conducted to replace the missing values with the mean value of each item.

3.5.2 Dependent Variable

The dependent variable "citizens' privacy concerns" has been measured to date by various survey questions in prior studies. While some researchers take responses given to only one survey question as a dependent variable, most of them take a group of questions to measure privacy concerns as a dependent variable. Drawing on the Harris-Westin Index, and reviewing Smith (2006) and Marqulis' (2010) choices of the GPD survey items, a latent variable was considered to be formed. Even though twelve items were considered initially for the formation of the dependent variable, later on, two items were removed because they did not meet the criteria of the reliability tests. Therefore, the dependent variable of the study was a latent variable composed of responses to ten survey questions each measuring citizens' privacy concerns and attitudes toward government surveillance, privacy, and security policies. The responses are presented using a Likert scale and ordinal level of measurement. These responses indicate the levels of concern ranging from low to high concerns. The twelve items that were considered at the beginning of the study, are indicated below along with the subsequent steps followed.

1. Trust in government about the right balance (q5)

-When it comes to the privacy of personal information, what level of trust do you have that your government is striking the right balance between national security and individual rights? (1 = Very high level of trust, 2 = Reasonably high level of trust, 3 = Fairly low level of trust, 4 = Very low level of trust, and 9=Not sure)

2. Intrusiveness of the laws protecting national security (q17)

-The government has enacted laws aimed at protecting national security. To what extent do you believe laws aimed at protecting national security are intrusive upon personal privacy? (1 = Highly intrusive, 2 = Somewhat intrusive, 3 = Not very intrusive, 4 =
Not intrusive at all, and 9=Not sure)

3. Government information sharing (q18)

-To what extent do you think it is appropriate for a government agency to share citizen's personal information with other government agencies?
-To what extent do you think it is appropriate for a government agency to share citizen's personal information with foreign governments?
-To what extent do you think it is appropriate for a government agency to share citizen's personal information with the private sector? (1 = Yes, it is the government's right under all circumstances 2 = Yes, if the citizen is suspected of wrong-doing 3 = Yes, as long as the government has the expressed consent of the citizen, 4 = No, under no circumstances should government share information about citizens, and 9= Not sure)

4. Airport privacy (q23)

-To what extent is your privacy respected by airport and customs officials when traveling by airplane? (1 = Completely respected, 2 = A lot of respected, 3 = Somewhat respected, 4 = Not respected at all, and 9 = Not sure)

5. Control over personal info (q2)

-To what extent do you have a say in what happens to your personal information? (1 = Complete say, 2 = A lot of say, 3 = Some say, 4 = No say, and 9 = Don't know/not sure)

6. Private information sharing (q19)

- To what extent do you think it is appropriate for a private organization to share or sell its customers' personal information with the national government?
-To what extent do you think it is appropriate for a private organization to share or sell its customers' personal information with foreign governments?
-To what extent do you think it is appropriate for a private organization to share or sell its customers' personal information with other private organizations? (1 = Yes, it is the organization's right under all circumstances 2 = Yes, if the customer is suspected of wrong-doing 3 = Yes, as long as the organization has the expressed consent of the citizen, 4 = No, under no circumstances should organizations share information about citizens, and 9= Not sure)

7. National IDs (q10)

-How effective do you feel government efforts to protect personal information required for issuing ID cards from disclosure would be? (1 = Very effective, 2 = Somewhat effective, 3 = Not very effective, 4 = Not effective at all, and 9 = Not sure)

8. Website privacy (q11)

-When it comes to privacy, how worried are you about providing personal information on websites, such as your name, address, date of birth, and gender? (1 = Very worried, 2 = Somewhat worried, 3 = Not very worried, 4 = Not worried at all, and 9 = Not sure)

Margulis (2010) and Smith (2006) considered those 12 items from the GPD survey which were consistent with the Harris-Westin Index. Therefore, following the strategy used by those scholars it was supposed that 12 items should be used to the desired construct privacy concern index. However, this theoretical argument has never been empirically tested. Based on this idea, the current study first subjected all 12 variables to a test of reliability to obtain their Cronbach's alpha scores. The results indicated that 12 variables fell short in constructing one reliable measure for privacy concern index (Cronbach's alpha= .65). Therefore, a further step-wise test of reliability was conducted, and each item was added to the scale after obtaining a reliability score at the threshold of (.70). In other words, the next item was added to the scale if the current scale already exceeded a Cronbach's alpha .70. When the addition of the new item from the pool of these 12 variables yielded a Cronbach's alpha score under .70, this item was excluded from the scale. The step-wise analysis resulted in 10 items with which to construct a reliable measure of privacy concern index with a Cronbach's alpha score (.70).

The "control over personal information (q2)" and the "website privacy (q11)" items were thus disregarded in the later stages of the research due to the stated reliability criteria. On the other hand, the "government information sharing (q18)" and "private information sharing (q19)" items both actually consisted of three components. Therefore, the dependent variable in total consisted of ten items.

Another consideration before the formation of the dependent variable was checking the answer choices in the items to establish whether they were in the correct order so that they would give meaningful results. Giving that the answer choices varied from one to four, the meaning of one had to resemble the least privacy concern, whereas the meaning

of the four had to reflect the highest privacy concern. The existing coding of the item "intrusiveness of the laws protecting national security (q17)" was not in the order that was desired. The number 1 was found to represent for the concept of being "highly intrusive", while the number 4 was used to indicate not "at all intrusive". Therefore, this item needed to be reverse-coded before starting the analyses. The other items forming the dependent variable were found to be listed in the right order.

3.5.3 Independent Variables

There were two types of independent variables in the study; the variables measured on the individual level and the variables measured at the country level and obtained from their original data sources. In order to make these suitable for the analysis, the variables measured at the country level were converted to individual level data by assigning country mean scores to every single individual who participated in the GPD survey.

3.5.3.1 Individual level Independent variables

The independent variable "Experience with surveillance measures" was measured by four questions that existed in the GPD survey. Those questions include (questions 8a, d, e, h):

- Have you personally, to the best of your knowledge, ever experienced detention:
  - at a border checkpoint resulting in a search?
  - by airport officials resulting in not being able to board the airplane?
  - by airport officials resulting in being denied entry into a country?
- Have you personally, to the best of your knowledge, your personal information monitored by a government agency? (1=Yes, 2=No, 9=Not sure)

The second independent variable "Knowledge of Laws" was measured by responses given to the two questions of the GPD survey. The respondents were asked about

their knowledge of laws that regulate personal information in government departments and private organizations:

-How knowledgeable are you about the laws in your country that deal with the protection of personal information

- in government departments?
- in private companies? (1=Very knowledgeable, 2=Somewhat knowledgeable, 3=Not very knowledgeable, 4=Not at all knowledgeable, 9=Don't know/unsure).

The "Perceived Media Coverage" variable is a composition of responses given to two separate questions. While the first asked about citizens' perceptions concerning the level of media coverage in terms of safety of personal information, the second, asks if the media cover more stories about terrorism, government's privacy violations, or an equal number of both. The second question represented a nominal level of measurement. Actual questions and answers include:

-How much coverage have you seen or heard through the media (TV, radio, newspapers, magazines, online information, advertisements) regarding concerns about the safety of your personal information?
(1=A lot of coverage 2=Some coverage 3=Not much coverage 4=No coverage at all, 9=Not sure)

-In your opinion, would you say the media pays: more attention to stories about terrorism/government violation of personal privacy of citizens/equal attention to both? (1= More attention to stories about terrorism, 2=More attention to stories about government violation of personal privacy of citizens, 3=Pays equal attention to both, 9=Not sure)

Factor analysis was performed to determine whether the variables experience with surveillance measures, knowledge of laws, and perceived media coverage have scale reliability. Since the items were believed to have been formed by reliable scales, a factor analysis was run. Results showed that they were not loaded into one factor and did not show reliable scales. Consequently they were kept as separate items in the analysis.

Four survey items measured the variable of "experience with surveillance measures". These were used as dummy variables. They asked about citizens experience with detention at a border checkpoint after a search, detention at an airport resulting not being able to board the airplane, a denial of entry into a country by airport officials, and if they experienced personal information monitoring by government agency. In the original data set the answers to this question were coded so that "1" meant "Yes" and "2" meant "No". However, these were first converted to a "0" that indicated "Yes" to the question and a "1" that indicated "No" to the question. Then they were reverse coded as "0" meaning "No" and "1" meaning "Yes" in order to ensure meaningful results from the statistical analyses.

Citizen's "knowledge of laws" was measured with two separate survey items. One of these two questions asked if individuals were knowledgeable about the laws regulating privacy and surveillance issues in government (public sector), whereas the other asked about the same level of knowledge in the private sector. The answers ranged from highly knowledgeable to not knowledgeable at all. However, the original answers were reverse coded again to rank order them from "1" meaning "not knowledgeable at all" to "4" meaning "highly knowledgeable".

Even it was assumed that the two items from the GPD Survey would form the variable "Media Coverage", the reliability scores of these two items indicated that they could not be constructed as one variable. On the other hand, the responses to one of the questions, consisted of 4 choice scales, while the other consisted of a 3 choice categorical scale. Therefore, these two items were included separately measuring the variable "media coverage" in the analysis.

The individual level dependent and independent variables were applied using the format that appeared in the original survey at the beginning of the variable formation process. However, when the analysis process started it was seen that they needed to be in a format where the higher score meant more of the variable. For instance, as stated above, the "knowledge of laws in government agency" variable was listed in the original data set with a 1 standing for "very knowledgeable" whereas a 4 was used for describing "not at all knowledgeable". This would have caused confusion in the statistical analysis process. Therefore, the relevant variables were reverse coded so that a higher score signified more of the variable.

3.5.3.2 Country Level Independent Variables

The fourth independent variable was related to one of the components of the dominant (cultural) values of a country. As a dominant value in a country the variable "confidence in government" was obtained from the WVS' Fifth Wave. The question in the survey appears with the code number V138 and the wording states; "I am going to name a number of organizations. For each one, could you tell me how much confidence you have in them: is it a great deal of confidence, quite a lot of confidence, not very much confidence or none at all?" Then one of the organizations listed was "the government in your nation's capital." Since trust is broadly discussed in the privacy literature, this question was considered to be a determinant of a national value that could affect attitudes to privacy and surveillance. The sample in the WVS was different from that of the GPD, therefore the individual level data was first converted into country level data by deriving the means of the countries, and then the mean values of each of the countries were assigned to represent the individuals in each respective country. The responses were listed using a Likert-type

scale where a "1" stood for "a great deal" and "4" stood for "none at all". The reverse coding strategy was also applied to this variable.

Another independent variable "Regime (Democracy Score)" listed using a 0 to 10 scale indicated that a 10 was the highest possible and best score. According to such a scoring system, countries were categorized under four regime types as follows; Full democracies (7.96 - 9.98), flawed democracies (5.98 – 7.91), hybrid regimes (4.01 – 5.91), and authoritarian regimes (1.03 – 3.92). Therefore, this level of measurement was an interval level. The US, Canada, France, Spain, Japan are listed under the full democracy category, Hungary and Brazil under the flawed democracies category, and China under the authoritarian regimes category (Kekic, 2007).

The sixth independent variable, the "impact of terrorism", was operationalized by defining a Global Terrorism Index (GTI). In order to measure the impact of terrorism, a country terrorism index score based on four indicators weighted over five years was developed. A unique scoring system was used to account for the relative impact of incidents in a given year. Each of the four factors was weighted between zero and three and a five year weighted average was calculated to reflect the psychological effect of terrorist acts over time. The total number of terrorist incidents, the total number of fatalities, the total number of injuries, and a measure of the total property damage from terrorist incidents in a given year were four factors taken into account in the calculation of the index. The greatest weight was given to fatality. The number of incidents was weighted with a one, the total number of fatalities was weighted with a three, the total number of injuries was weighted with 0.5, and the sum of the property damages measure was weighted depending on the severity between zero and three. The time weighting going back five years in history

was done by using the following criteria; current year 52%, previous year 26%, two years ago 13%, three years ago 6%, and four years ago 3%. The final country scores employ a scale of 0 to 10. The higher number is the worst case in terms of terrorism impact. The GTI scores were considered since they are expected to reflect the psychological and emotional effects of terrorism incidents (IEP, 2014).

The "Regulations (Privacy Index)" variable was considered initially to be both an independent and dependent variable in the study. It was regarded as an independent variable because it might affect citizens' privacy concerns. The privacy regulations issue may come first and predict the citizens' privacy concerns. On the other hand, privacy concerns may lead to further tensions and as a result, governments may consider altering certain privacy regulations. It can be inferred from Smith et al.'s (2011) APCO macro model that "regulations" can be both antecedent and outcome. If we want to examine whether the process of public policy formation pays attention to citizens' privacy concerns, this renders the "regulations" variable, a dependent variable. However, with the data in hand having only 8 country variations of privacy regulations, it is not possible to employ the privacy regulations variable both as dependent and independent variable at the same time. Therefore, it was decided to use the privacy regulations variable solely as an independent variable in the statistical analysis.

Individual country laws and other sources of regulation regarding privacy and surveillance were reviewed and reported by country reporters. Then country reports were evaluated according to fourteen criteria and rates were provided by legal, technical, and academic experts. Later the average of fourteen criteria was calculated and determined as a country privacy index. It was operationalized by expert's evaluations of privacy and

surveillance regulations in the various countries. The scores reflect the numbers 1 to 5 on a scale and this represented an interval level of measurement determining whether the country in question had endemic surveillance (score 1.1 to 1.5) or good protection of human rights of its citizens (4.1 to 5.0). The data used was that provided for the year 2007. In 2010, the evaluation criteria were increased to seventeen criteria and the evaluation of privacy regulations was carried out only for European countries according to a one to ten point scale. However this study considered taking the previous -2007 rankings of Privacy Index- scores which were compatible with the countries of interest and the years of the remaining data sources. The Privacy Index was unique since it is the only existing cross-national evaluation of privacy regulations (EPHR Report, 2011: Privacy International, 2014).

Table 3.2. List of the Evaluation Criteria for Privacy Index 2007

(Privacy International, 2014)

•Constitutional protection	•Workplace monitoring
•Statutory protection	•Government access to data
•Privacy enforcement	•Communications data retention
•Identity cards and biometrics	•Surveillance of medical, financial and movement
•Data-sharing	•Democratic safeguards
•Visual surveillance	•Border and trans-border issues
•Communication interception	•Leadership

Table 3.3. Study Variables, Their Levels, and Sources

Dependent/ Independent	Variables	Level of Data	Source of Data	Question #
D.V.	Privacy/Surveillance Concern	Individual	Globalization of Personal Data Survey (GPD) 2006	Q5, 17, 18,19,23,10
I.V.	Experience With Surveillance Measures	Individual	GPD 2006	Q8.a,d,e,h
I.V.	Knowledge of Laws	Individual	GPD 2006	Q3.a,b
I.V.	Perceived Media Coverage	Individual	GPD 2006	Q13, 14
I.V.	Cultural Value (Confidence to Government)	Country	World Values Survey 5th Wave 2005-2009	V138
I.V.	Regime (Democracy Score)	Country	The Economist Intelligence Unit - 2006	
I.V.	Impact of Terrorism (Global Terrorism Index)	Country	Institute for Economics and Peace (IEP) - 2006	
I.V.	Regulations (Privacy Index Score)	Country	Privacy International - 2007	
I.V.= Independent Variable D.V.= Dependent Variable				

CHAPTER IV

ANALYSES AND FINDINGS

4.1 Statistical Models Used in the Analysis

Several statistical tests were performed for the analysis of the data. These included Pearson Correlation, T-test, one-way ANOVA, Chi-square tests, and Ordinary Least Square (OLS) Regression.

For the bivariate analysis, a one-way ANOVA test was appropriate for investigating the mean differences across countries because the variable of nationality has more than two categories and the other variables including knowledge of laws, cultural values, regime, impact of terrorism, perceived media coverage, and regulations are continuous. The T-test was used for the questions with yes/no answers, or those with a relationship between continues and dummy variables. The chi-square test was run when the independent and dependent variables were both categorical variables.

For the multivariate analysis, OLS Regression test was run. The OLS Regression test is appropriate for investigating the effects of the independent variables including experience with surveillance measures, knowledge of laws, confidence to government, regime, impact of terrorism, perceived media coverage, and regulations on the dependent variable of privacy concern because the independent and the dependent variables are continuous.

The statistical analysis of the study began with descriptive statistics, (see results in Table 4.1 below), then continued with bivariate analysis of independent variables and the dependent variable, citizen privacy concerns. In addition, cross-country variations of all

variables was measured through bivariate analyses. Finally, multivariate analysis was conducted by clustering independent variables according to countries included in the study.

Table 4.1. Descriptive Statistics for Dependent and Independent Variables

Descriptive Statistics		Mean	Min	Max
Dependent Variable (N=8526)				
Citizens' Privacy Concern		2.75	1.23	3.8
Independent Variables				
Individual Level Variables (N=8526)				
Knowledge of Laws				
Knowledge of Laws (in government)		2.15	1	4
Knowledge of Laws (in private)		2.06	1	4
Experience With Measures:				
Border Checkpoint	(Y=928, N=7521)	.11	0	1
Boarding Plane	(Y=703, N=7553)	.08	0	1
Denial of Entry	(Y=576, N=7876)	.07	0	1
Monitored by Government	(Y=1456, N=5865)	.20	0	1
Media Coverage:				
Coverage on Personal Info Safety		2.50	1	4
Coverage on Terror/Gov Violation/Both		2.03	1	3
Country Level Variables (N=8)				
Privacy Regulations		2.04	1.3	2.9
Democracy Score		6.90	2.97	9.07
Terrorism		2.07	0	5.62
Confidence in Government		2.44	1.74	3.32

4.2 Bivariate Analysis

There are two level of variables in the data set. There are eight variables at the individual level and four variables at the country level. The sample size for the individual-level variables was 8,526, but the sample size for the country-level variables was only 8. This had some implications and drawbacks for analysis at the bivariate level. The bivariate correlations regression results were statistically reliable because there was enough

variation in the data set, but that was not the case for the country-level variables. Bivariate correlation results between individual-level independent variables and the dependent variable are shown in the Table 4.2. In addition, bivariate analysis also was done for country-level variables and is shown in the Table 4.2.

Table 4.2. Bivariate Correlation between Dependent and Independent Variables (Individual and country level variables)

Bivariate Analysis		
Independent Variables		**Dependent Variable**
Individual Level Variables (N=8526)		Citizen Privacy Conc
Knowledge of Laws[P]:		
Laws in Government		n.s.
Laws in Private Sector		n.s.
Experience With Measures[T]:		
Border Checkpoint	(Y=928, N=7521)	**1.54***
Boarding Plane	(Y=703, N=7553)	n.s.
Denial of Entry	(Y=576, N=7876)	**2.16****
Monitored by Government	(Y=1456, N=5856)	**6.53****
Media Coverage:		
Coverage on Personal Info Safety[P]		n.s.
Coverage on Terror/Govt Violation/Both[F]		**3.33****
Country Level Variables		
Privacy Regulations		**-0.06****
Terrorism		n.s.
Democracy Score		**-0.05****
Confidence in Gov.		**-0.08****

**α<0.05, *α<0.10

T= indicates T-Test results

F= indicates ANOVA results

P= indicates Pearson's correlations results

4.2.1 Test of Hypotheses at the Individual Level

H_1: The "knowledge of laws" variable consisted of two survey items, and the relationship to citizens' privacy concern was tested using two Pearson's Correlation tests. It was found that both knowledge of laws in the private sector and knowledge of laws in the government (public sector) were not significantly associated with privacy concerns (H_1-a, H_1-b).

H_2-a: Pearson's Correlation test results for exposure to media coverage related to safety of personal information indicated that this association was not statistically significant. In this study, more exposure to the media was not correlated with more concern for privacy, on average.

H_3-a: The relationship between the dependent variable "citizen privacy concerns" and four items of the independent variable "experience with surveillance measures" were tested with the t-test. One of the hypotheses of this study posited that an experience with detention at a border checkpoint after a search would increase privacy concern. The difference in mean privacy concern between the groups of participants who reported that they experienced detention at a border checkpoint after a search in the past and those who did not was statistically significant ($t=1.5439$, $p<.10$). On average, those who were detained in the past reported higher privacy concern. Therefore, the association between these two variables was supported by the results from the sample.

H_3-b: This hypothesis that the "experience with the detention from boarding on an airplane" will be positively associated with "privacy concern" was also tested though t-test. However, the difference in mean privacy concern between the groups of participants who reported that they experienced the detention when boarding on an airplane in the past and

those who did not have this experience was not statistically significant. Therefore, the association between these two variables was not supported by the results from this sample.

H_3-c: The hypothesis about experience with surveillance measures posited that "the detention at the airport resulting in denial of entry" would be positively associated with "privacy concern". Likewise, the difference in mean privacy concern between the groups of participants who reported that they were detained at an airport and denied entry into a country and those who did not have this experience in the past was statistically significant ($t=2.1648$, $p<.05$). On average, those who were detained in the past reported higher privacy concern. Therefore, the association between those two variables was supported by results from this sample.

H_3-d: The hypothesis that the experience with "personal information monitored by government" would increase privacy concerns was also tested with t-test. As expected, there was a statistically significant difference in mean privacy concern between the groups of participants who reported that their personal information was monitored by government and those who reported not having such an experience in the past ($t=6.5286$, $p=0.000$). More specifically, those with previous experience of being monitored by the government reported more privacy concern on average

H_2-b: The hypothesis that privacy concern would differ among the group of participants who perceive a difference in the attention of the media was tested with ANOVA. The variable examining the citizen's perceptions about the stories they see on the media included three categories. These categories consisted of the expressions that the media pays more attention to stories about: "terrorism", "government violation of personal privacy of citizens", and "equal attention to both". This variable is not an ordinal level variable, and

there is not a hierarchy among the attributes. Therefore, ANOVA was used to analyze the potential mean difference across those three groups. The ANOVA test results indicated that there was a statistically significant difference among three groups in respect for privacy concern ($F=3.33$, $df=2, 8518$, $p<.05$). To unfold which group was significantly different from the others, a further post hoc test (Bonferronni) was conducted. The results showed that, on average, the privacy concern of those who reported that both stories are more on the media was significantly higher than that of those who reported that news on government violation of privacy take more place in the media.

4.2.2 Test of Hypotheses at the Country Level

H_4, H_5, H_6, and, H_7 were tested at the country level with Pearson's Correlation test.

H_4: The hypothesis that the dominant cultural values in a country (confidence in government) are associated with citizens' privacy concerns found support in this study since the variables were significantly correlated ($r=-0.08$, $p< 0.05$).

H_5: The hypothesis that a higher emotional experience with terrorism is negatively associated with privacy concerns was not supported at the bivariate level since the variables were not significantly correlated.

H_6: The hypothesis that the higher the democracy score of a country the lower would be the citizens' privacy concerns was supported with a significant correlation between variables ($r=0.05$, $p< 0.10$).

H_7: The privacy regulations were expected to be in association with the citizens' privacy concerns in respective countries. When we looked at the correlation between privacy regulation and privacy concerns, there was a negatively significant but weak relationship

between two variables (r=-0.06, p< 0.10). The less the quality of privacy regulations was the more citizen privacy concerns.

The privacy regulations variable was further analyzed because this dissertation project was also interest in the relationship between the regulations and privacy concerns. The extant literature suggested that the regulations are both antecedent and outcome, thus, two way relationship with privacy concern might exist. However, the current data on the "privacy regulations" were not adequate to test this two-way relationship. Therefore, the bivariate analysis only examined the relationship of the privacy regulations to the "citizens' privacy concern" by pairwise correlation, and then, a table of cross-country comparison was produced. The regulations variable was also tapped into the multivariate model, which will be discussed in the following pages.

Figure 4.1. Comparison of Privacy Index (Privacy Regulations) and Privacy Concerns

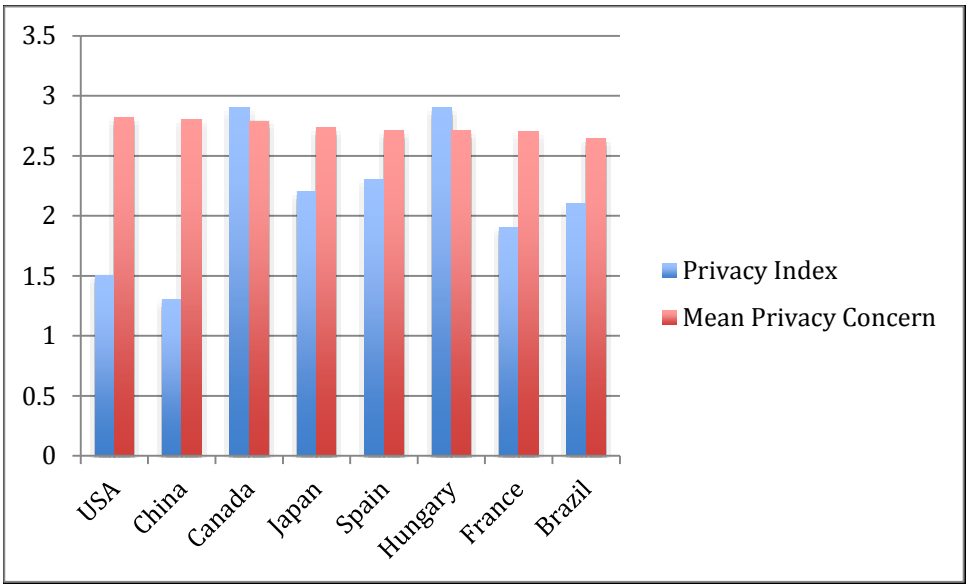


Table 4.3. Country Means of Privacy Index and Privacy Concerns

Country	Privacy Index	Mean Privacy Concern
USA	1.5	2.815
China	1.3	2.799
Canada	2.9	2.789
Japan	2.2	2.736
Spain	2.3	2.708
Hungary	2.9	2.707
France	1.9	2.706
Brazil	2.1	2.645

4.2.3 Country Level Variation in All Variables

As this study used country level variables to understand whether different contexts are related to different levels of privacy concerns, it was important to first analyze variations in the dependent variable at eight countries and then examine other country-level variables. The analysis of variance (ANOVA) test enables the analysis of this variation. However, the date in this study did not allow to obtain ANOVA test results for the variables democracy score, terrorism, privacy regulations, and confidence in government because there was only 8 observations, and thus very small variation in these four variable.

H_9: The hypothesis posited that citizens' privacy concerns vary across countries. This hypothesis was tested using ANOVA because the dependent variable was continuous and the independent variable was categorical (i.e., countries). The test results indicated that the dependent variable "citizens' privacy concerns" differs statistically significantly by country ($F=24.39$, $df =7/8518$, $p<0.000$). In other words, citizens of eight different countries reported different levels of privacy concerns on average. Such a finding and conclusion lends support for the further analysis of the relationship between privacy concern and other independent variables at both individual and country levels.

The Table 4.4 shows that the citizens of the US, on average, were found to have the most privacy concerns (M=2.82; SD=.40), followed by the China, Canada, Japan, Hungary, France, Spain and Brazil. The citizens of Brazil were found to have the least privacy concerns (M=2.64; SD=.49) among the eight countries.

Table 4.4. One-way ANOVA Citizen Privacy Concerns by Countries

	N	Mean	SD
United States	1000	2.82	0.40
China	2002	2.80	0.36
Canada	1001	2.79	0.39
Japan	516	2.74	0.41
Hungary	1005	2.73	0.35
France	1002	2.71	0.38
Spain	1000	2.71	0.44
Brazil	1000	2.64	0.49

F=24.39; df=7/8518; p=0.000

Table 4.5. Comparison of Citizen Privacy Concern by Country (Bonferroni)

	Brazil	Canada	China	France	Hungary	Japan	Spain
Canada	**0.144**						
	0.000						
China	**0.154**	0.010					
	0.000	1.000					
France	**0.061**	**0.083**	**0.094**				
	0.019	**0.000**	**0.000**				
Hungary	**0.062**	**0.082**	**0.092**	0.002			
	0.013	**0.000**	**0.000**	1.000			
Japan	**0.091**	0.053	**0.063**	0.031	0.029		
	0.001	0.413	**0.038**	1.000	1.000		
Spain	**0.063**	**0.081**	**0.091**	0.002	0.001	0.028	
	0.012	**0.000**	**0.000**	1.000	1.000	1.000	
USA	**0.170**	0.027	0.016	**0.110**	**0.108**	**0.079**	**0.108**
	0.000	1.000	1.000	**0.000**	**0.000**	**0.007**	**0.000**

The comparison table above (Table 4.5) indicates that, when countries are paired, the privacy concerns between the citizens of some countries were found to be different from each other, whereas in other pairs of countries privacy concerns of citizens did not differ from each other. As shown in the Table 4.5, China and Canada, Hungary and France, Japan and Canada, Japan and France, Japan and Hungary, Spain and France, Spain and Hungary, Spain and Japan, the USA and Canada, and the USA and China were wound to not differ significantly in terms of citizen privacy concerns. The remaining bivariate relationships between countries were found to be different from each other. These findings will be discussed in the next chapter.

H_8: The hypothesis that privacy regulations vary across 8 countries was tested by ANOVA. Though privacy regulations, operationalized by privacy index, varied across countries, ANOVA test results were not obtained because there was only 8 observations, and thus very small variation in this variable. Therefore, the country indexes of privacy regulations are shown in the Table 4.6. This is also the case for the other country variables -confidence in government, terrorism, and regime type. Table 4.6 illustrates that the country with the highest score of privacy regulations is Canada, whereas China has the lowest score.

Table 4.6. Privacy Regulations (Privacy Index) by Country

Country	Mean	Freq.
Canada	2.9	1001
Hungary	2.9	1005
Spain	2.3	1000
Japan	2.2	516
Brazil	2.1	1000
France	1.9	1002
USA	1.5	1000
China	1.3	2002
Total	2.036	8526

H_{10}: The hypothesis that the correlates of privacy concerns vary across 8 countries required to conduct bivariate statistical analyses based on the level of measurement of each of 11 correlates.

The democracy score of a country is one of the indicators of regime type. As seen in Table 4.7 below, the data revealed that Canada had the highest democracy score of the countries included in the study. On the other hand, China was found to have the lowest

democracy score. According to source of democracy scores, there were four categories: Full democracies, flawed democracies, hybrid regimes, and authoritarian regimes (Kekic, 2007). Countries included in the analysis fell into three categories: Full democracies, which included the first five countries in Table 4.7; flawed democracies, which included Hungary and Brazil; and, finally, authoritarian regimes, which included China.

Table 4.7. Regime (Democracy Score) by Country

Country	Mean	Freq.
Canada	9.07	1001
Spain	8.34	1000
USA	8.22	1000
Japan	8.15	516
France	8.07	1002
Hungary	7.53	1005
Brazil	7.38	1000
China	2.97	2002
Total	6.90	8526

Table 4.8 illustrates the level of confidence by countries. The country with the highest level of confidence in government was China whereas the country with the lowest level of confidence in government was Hungary.

Table 4.8. Confidence in Government by Country

Country	Mean	Freq.
China	3.32	2002
Spain	2.37	1000
Brazil	2.34	1000
USA	2.32	1000
Canada	2.30	1001
Japan	2.14	516
France	2.01	1002
Hungary	1.74	1005
Total	2.44	8526

Table 4.9 displays terrorism scores for each of the countries in the study. It shows that Spain was at the highest end of the spectrum, and Hungary was at the lowest end of the emotional experience with terrorism.

Table 4.9. Terrorism Index by Country

Country	Mean	Freq.
Spain	5.62	1000
USA	3.38	1000
France	2.32	1002
Brazil	1.97	1000
China	1.56	2002
Canada	1.16	1001
Japan	0.1	516
Hungary	0	1005
Total	2.07	8526

It was hypothesized that correlates of citizens' privacy concerns which were individual-level variables, vary across countries. The variation of these variables was tested

with ANOVA as well. There were eight individual-level variables organized in three categories, including experience with surveillance measures, knowledge of laws, and media coverage.

Table 4.10 illustrates that citizens of Hungary were less knowledgeable about laws regulating personal information privacy in government, whereas the citizens of the US were seen to be most knowledgeable. Citizens' knowledge of laws in government significantly differ across countries.

Table 4.10. Knowledge of Laws in Government by Country

Country	Mean	Std. Dev.	Freq.
USA	2.48	0.84	1000
Canada	2.38	0.88	1001
France	2.22	0.77	1002
China	2.16	0.77	2002
Spain	2.12	0.9	1000
Japan	2.09	0.67	516
Brazil	1.91	0.93	1000
Hungary	1.81	0.78	1005
Total	2.15	0.86	8526

F=66.98; df=7/8518; p=0.000

Table 4.11. Comparison of Citizen Knowledge of Laws in Government by Country (Bonferroni)

	Brazil	Canada	China	France	Hungary	Japan	Spain
Canada	**-0.46** **0.00**						
China	**-0.24** **0.00**	**0.22** **0.00**					
France	**-0.30** **0.00**	**0.15** **0.00**	-0.06 1.00				
Hungary	0.10 0.15	**0.56** **0.00**	**0.34** **0.00**	**0.41** **0.00**			
Japan	**-0.17** **0.00**	**0.28** **0.00**	0.06 1.00	0.13 0.13	**-0.28** **0.00**		
Spain	**-0.20** **0.00**	**0.26** **0.00**	0.04 1.00	0.10 0.19	**-0.30** **0.00**	-0.03 1.00	
USA	**-0.55** **0.00**	-0.10 0.26	**-0.32** **0.00**	**-0.25** **0.00**	**-0.66** **0.00**	**-0.38** **0.00**	**-0.35** **0.00**

Table 4.11 above shows that, the citizens' knowledge of laws in government are same in posthoc comparison among some countries whereas different among other. Bonferroni test results in 4.11 indicates that the following paired countries were not significantly different from each other in terms of citizens' knowledge of law in public sector. Those pairs of countries were France and China, Hungary and Brazil, Japan and China, Japan and France, Spain and China, Spain and France, Spain and Japan, and US and Canada.

Table 4.12. Knowledge of Laws in Private Sector by Country

Country	Mean	S D	N
USA	2.41	0.85	1000
Canada	2.24	0.84	1005
Japan	2.14	0.68	516
China	2.08	0.79	1000
Spain	2.06	0.99	2002
France	2.01	0.77	1002
Hungary	1.82	0.79	1000
Brasil	1.78	0.90	1000
Total	2.06	0.85	8526

F=59.90; df=7/8518; p=0.000

Table 4.12 above shows that the citizens of the US are the most knowledgeable about the privacy laws that apply to private sector whereas the citizens of Brazil are less knowledgeable about such privacy laws.

Table 4.13. Comparison of Citizen Knowledge of Laws in Private Sector by Country (Bonferroni)

	Brazil	Canada	China	France	Hungary	Japan	Spain
Canada	**-0.45**						
	0.00						
China	**-0.29**	**0.16**					
	0.00	**0.00**					
France	**-0.22**	**0.23**	0.07				
	0.00	**0.00**	0.96				
Hungary	-0.03	**0.42**	**0.26**	**0.19**			
	1.00	**0.00**	**0.00**	**0.00**			
Japan	**-0.34**	0.11	-0.06	-0.13	-0.31		
	0.00	0.49	1.00	0.15	0.00		
Spain	**-0.27**	**0.18**	0.02	-0.05	**-0.24**	0.08	
	0.00	**0.00**	1.00	1.00	**0.00**	1.00	
USA	**-0.62**	**-0.17**	**-0.33**	**-0.40**	**-0.59**	**-0.27**	**-0.35**
	0.00	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**

Table 4.13 indicates that the following pairs of countries were not significantly different from each other in terms of citizens' knowledge of laws in private sector. Those pair of countries were France and China, Hungary and Brazil, Japan and Canada, Japan and China, Japan and France, Spain and China, Spain and France, and Spain and Japan.

Table 4.14. Media Coverage about Safety of Personal Information Privacy by Country

Country	Mean	Std. Dev.	Freq.
USA	3.12	0.73	1000
China	2.80	0.80	2002
Canada	2.77	0.74	1001
Japan	2.26	0.65	516
Hungary	2.19	0.81	1005
Spain	2.19	0.90	1000
Brazil	2.16	0.99	1000
France	2.08	0.74	1002
Total	2.50	0.86	8526

F=226.30; df=7/8518; p=0.000

According to the Table 4.14, the citizens of the US reported to see the most media coverage about safety of personal information privacy. On the other hand, citizens of France reported the least media coverage about safety of personal information privacy.

Table 4.15. Comparison of Media Coverage about Safety of Personal Information Privacy by Country (Bonferroni)

	Brazil	Canada	China	France	Hungary	Japan	Spain
Canada	**-0.55**						
	0.00						
China	**-0.62**	-0.06					
	0.00	0.96					
France	0.04	**0.60**	**0.66**				
	1.00	**0.00**	**0.00**				
Hungary	-0.05	**0.51**	**0.57**	-0.09			
	1.00	**0.00**	**0.00**	0.28			
Japan	-0.10	**0.45**	**0.52**	**-0.15**	-0.05		
	0.50	**0.00**	**0.00**	**0.02**	1.00		
Spain	-0.04	**0.52**	**0.58**	-0.08	0.01	0.06	
	1.00	**0.00**	**0.00**	0.60	1.00	1.00	
USA	**-0.89**	**-0.34**	**-0.27**	**-0.93**	**-0.84**	**-0.79**	**-0.85**
	0.00	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**

The correlations between pairs of countries depicted in Table 4.15 show that the following pairs of countries do not differ in terms of reported media coverage about safety of personal information privacy: China and Canada, France and Brazil, Hungary and Brazil, Hungary and France, Japan and Brazil, Japan and Hungary, Spain and Brazil, Spain and France, Spain and Hungary, and Spain and Japan.

The variation across countries for four correlates of privacy concern was tested by Chi-square test since these variables were categorical. In this sample, the first Chi-Square test examined if there was a relationship between countries and the type of media coverage that their citizens were exposed. One of the media coverage variables had three categories

and the country variable was also taken as an eight-category variable. Another categorical variable was the experience with surveillance measures. The experience with surveillance measures consists of four separate, two category variables. The results of Chi-square analysis showed that there is statistically significant relationships between countries and citizens' opinion about what media pay more attention in their countries (X^2 =2.12.; df=21; p= 0.000). Missing values were not included in the table.

Table 4.16. Chi-Square Test between Country and Type of Media Coverage

Media Coverage:	Brazil	Canada	China	France	Hungary	Japan	Spain	USA	Total
Media pays more attention to terrorism	528 52.8	497 49.65	185 **9.24**	400 39.92	332 33.03	112 21.71	627 **62.7**	356 35.6	3,037 35.6
Media pays more attentn to govt violation of priv.	141 14.1	28 **2.8**	479 **23.93**	35 3.49	83 8.26	60 11.63	42 4.2	107 10.7	975 11.4
Equal attention to both	257 25.7	230 22.98	1,253 **62.59**	339 33.83	410 40.8	249 48.26	218 **21.8**	296 29.6	3,252 38.1
Total	1000 100	1001 100	2002 100	1002 100	1005 100	516 100	1000 100	1000 100	8526 100

Pearson chi2(21) = 2.12 Pr = 0.000

In the Table 4.16 and following chi-square tables the highest and the lowest percentages in the row were marked in bold. For instance, in Table 4.16 above, 62.7% percent of the Spanish citizens reported that the media pay more attention to terrorism while Chinese citizens reported the lowest media coverage about terrorism. This outcome is also consistent with the terrorism index of Spain, which was also found to be the highest among the other countries included in the study. On the other hand, citizens of China reported more media coverage on the remaining two categories (government violation of

personal information privacy and equal attention to both terrorism and government violation of personal information privacy) than others.

Table 4.17. Chi-Square Test between Country and Experience of Detention from Search at Border Checkpoint

Experience of detention from search at border checkpoint	Brazil	Canada	China	France	Hungary	Japan	Spain	USA	Total
Yes	17	169	53	217	236	39	71	126	928
	1.70	16.88	2.65	21.66	**23.48**	7.56	7.10	12.60	10.88
No	983	819	1941	783	765	451	925	854	7521
	98.30	81.82	96.95	78.14	**76.12**	87.40	92.50	85.40	88.21
Total	1000	1001	2002	1002	1005	516	1000	1000	8526
	100	100	100	100	100	100	100	100	100

Pearson chi2(14) = 713.14 Pr = 0.000

Table 4.18. Chi-Square Test between Country and Experience of Detention Resulting in Not Being Able to Board the Airplane

Experience of detention, not being able to board airplane	Brazil	Canada	China	France	Hungary	Japan	Spain	USA	Total
Yes	69	69	235	70	56	11	50	143	703
	6.90	6.89	11.45	6.99	5.57	**2.13**	5.00	**14.30**	8.25
No	928	904	1752	911	865	480	900	813	7553
	92.80	90.31	87.51	90.92	86.07	93.02	90.00	81.30	88.59
Total	1000	1001	2002	1002	1005	516	1000	1000	8526
	100	100	100	100	100	100	100	100	100

Pearson chi2(14) = 309.09 Pr = 0.000

Table 4.19. Chi-Square Test between Country and Experience of Detention Resulting in Being Denied Entry into a Country

Experience of detention at airport, denied entry	Brazil	Canada	China	France	Hungary	Japan	Spain	USA	Total
Yes	28	139	67	86	13	16	54	173	576
	2.80	13.89	3.35	8.58	**1.29**	3.10	5.40	**17.30**	6.76
No	971	855	1926	914	983	481	942	804	7876
	97.10	85.41	96.2	91.22	97.81	93.22	94.20	80.40	92.38
Total	1000	1001	2002	1002	1005	516	1000	1000	8526
	100	100	100	100	100	100	100	100	100

Pearson chi2(14) = 479.45 Pr = 0.000

Table 4.20. Chi-Square Test between Country and Experience of Personal Information Being Monitored by a Government Agency

Personal info. monitored by government agency	Brazil	Canada	China	France	Hungary	Japan	Spain	USA	Total
Yes	21	236	295	174	122	64	204	340	1,456
	2.10	23.58	14.74	17.37	12.14	12.40	20.40	**34.00**	17.08
No	965	602	1612	713	630	303	599	441	5865
	96.50	60.14	80.52	71.16	62.69	58.72	59.90	44.10	68.79
Total	1000	1001	2002	1002	1005	516	1000	1000	8526
	100	100	100	100	100	100	100	100	100

Pearson chi2(14) = 1.12 Pr = 0.000

The data displayed in Table 4.20 shows that a statistically significant relationship was found between countries and citizens with experience having their personal information monitored by government agency. The citizens of the US (34%) and Canada (23.58%) are the most experienced with having their personal information monitored by the government. On the other hand, citizens of Brazil and Japan were found to be the least

exposed to the experience of having their personal information monitored by government. In addition, in all of the chi-square tables above, except one, the US scored high in terms of experience with surveillance measures, which strengthens the notion of the "surveillance state."

4.3 Multivariate Analysis

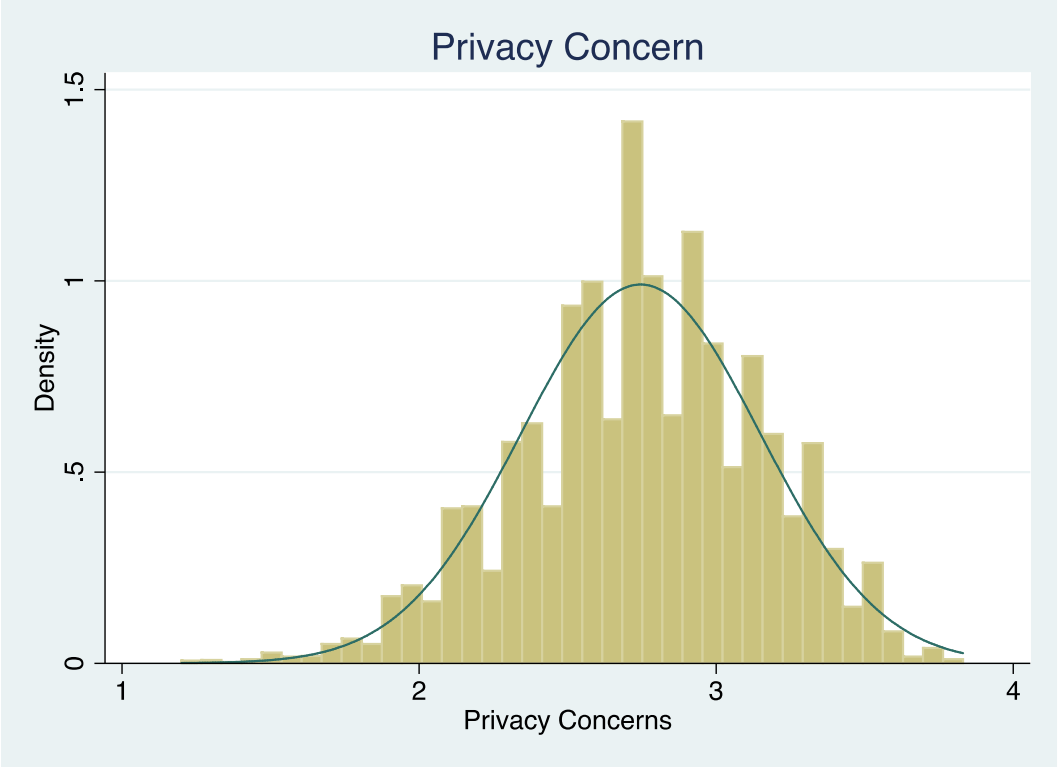
4.3.1 Sensitivity Analysis

The current study uses Ordinary Least Squares (OLS) Regression for the multivariate analysis. There are several assumptions to test before beginning the OLS modeling. Therefore a sensitivity analysis was conducted to understand whether the dependent variable and residuals were normally distributed in the dataset, whether the dependent and independent variables were linear, and if there was a multicollinearity problem for the variables.

4.3.2 Test for Normality

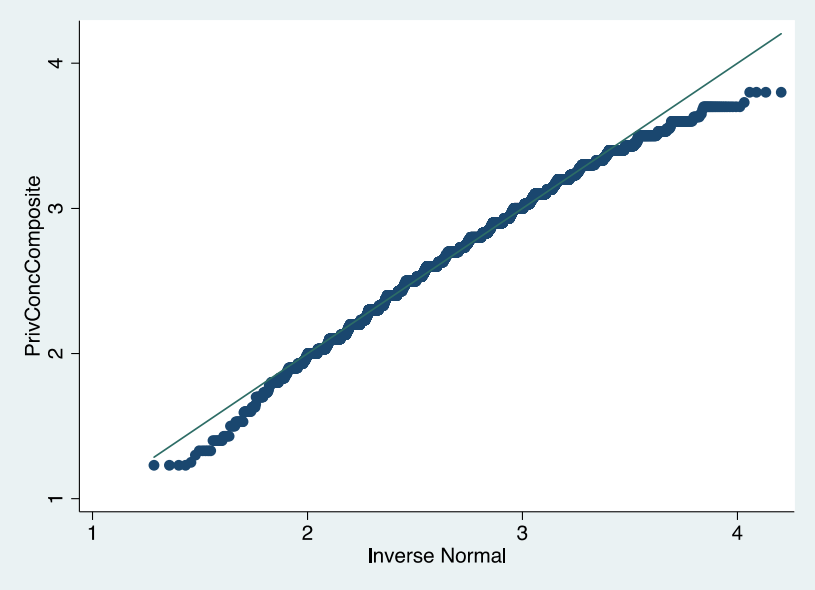
A visual inspection of the distribution of the dependent variable "citizen privacy concerns" suggested that the distribution of the dependent variable was normal with a bell shape.

Table 4.21. Histogram: The Distribution of the Dependent Variable



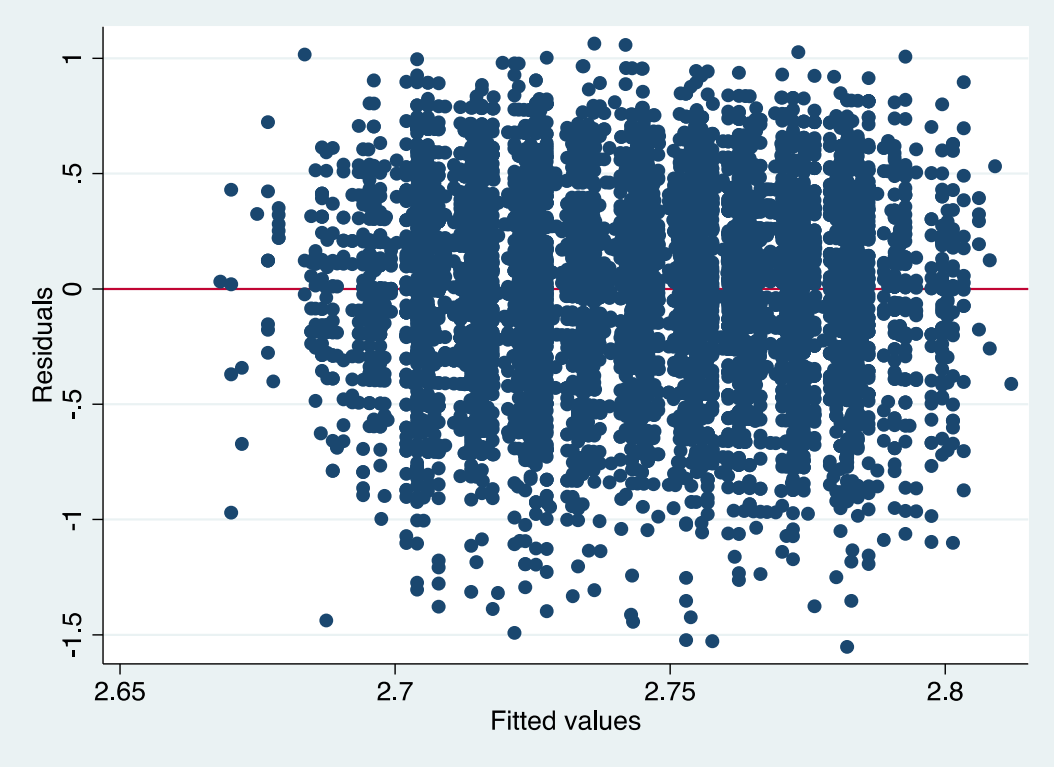
Qnorm command in STATA helps understand the degree to which a distribution is normal. In the next step, the linearity between the dependent variable and each of independent variables was separately probed. The augmented component plus residual test was conducted for this reason and neither a quadratic nor a polynomial relationship was observed between variables that were not dichotomous.

Table 4.22. Residual Test



Another assumption is that variance of the residuals should be normal in the regression model. In other words, "the variation of the dependent variable around the regression surface is everywhere the same" (Fox, 1991 p.49). This is also called the homoscedasticity of the residuals. To further analyze the normality issue, the dependent variable was regressed on individual level variables. Then, the residuals from the model was predicted and a new variable was created for standard errors. In the next step, the residuals were plotted against the fitted values on a scatter plot. The resulting scatter plot suggested that the distribution of residuals was acceptable and normally distributed with a fan shape. However, robust standard errors were used to adjust the model for heteroscedasticity, which enables the correct estimation of residuals and the avoidance of misguided coefficients and significance (Fox, 1991).

Table 4.23. Residuals vs. Fitted Values Plot



The data set was also examined in respect for outliers. No outliers were observed in the data set after a regression of dependent variable on the individual-level independent variables.

4.3.3 Multicollinearity Test

The Variance Inflation Factors (VIF) tolerance scores ranged between 1.04 and 1.58, and the average VIF value was 1.20. The VIF values were below 2.00; therefore, the conclusion was that multicollinearity was not a problem with the variables in the model.

4.3.4 Model Specification

The current study was mainly interested in the relationship between the citizen privacy concerns and the antecedents of these concerns emphasized in the literature, and

assumes that they may vary across eight countries. Therefore, a two-step analytic strategy was adopted. First, the variation in the dependent variable across the eight countries was examined with ANOVA, as explained in the bivariate analysis section above, and then all antecedents of privacy concerns were simultaneously modeled to determine their anticipated influences, which is explained in the present section on multivariate analysis.

4.3.5 Multiple Regression

Table 4.24. Multiple Regression Analysis of Antecedents of Privacy Concerns to Citizen Privacy Concerns

Independent Variables	Coef.	Std. Err.	t	P>|t|	[95%	Conf. Interval]
Know Law Govt	.005	.006	0.72	0.492	-.010	.019
Know Law Private	**-.014**	**.005**	**-2.81**	**0.026****	**-.025**	**- .002**
Media Pers Info S	-.010	.007	-1.35	0.218	-.027	.007
Media Ter/Viol/Both	-.001	.009	-0.13	0.902	-.023	.020
Border checkpoint	**.031**	**.014**	**2.15**	**0.069***	**-.003**	**.065**
Boarding airplane	-.005	.015	-0.33	0.748	-.040	.030
Denial of entry	.024	.016	1.50	0.178	-.014	.062
Govt. monitor privacy	**.084**	**.018**	**4.57**	**0.003*****	**.040**	**.127**
Confidence in Govt.	**.153**	**.043**	**3.51**	**0.010****	**.049**	**.256**
Terrorism	**-.017**	**.004**	**-3.64**	**0.008*****	**-.029**	**-.006**
Democracy	.025	.013	1.87	0.104	-.006	.057
Privacy Regulations	-.025	.039	-0.64	0.546	-.119	.068
_cons	2.307	.154	14.97	0.000	1.942	2.671

p< .10*, p<.05**, p<.01*** R-squared = .017 N=8526

Table 4.24 demonstrates the results of the Ordinary Least Square (OLS) model that included all individual and country level variables. The results of the multivariate analysis

showed that there were some differences between bivariate and multivariate analyses. At the bivariate analysis, two individual level variables were significantly related to the privacy concern. These variables were the "exposure to media coverage on both terrorism and violence" (Media Ter/Viol/Both) and the "experience of surveillance measures on denial of entry at the airport" (Denial of Entry). However, they were no longer significant in the multivariate model. Though another individual-level independent variable - "knowledge of laws in private sector"- was not significant at the bivariate analysis, it came up as significant.

The independent variable, "knowledge of laws" regulating privacy in private sector was statistically significant in the OLS model, but the relationship was not in the expected direction ($b=-0.14$, $t=2.81$, $p<0.05$). Controlling for the other independent variables, those who were more knowledgeable of law stated, on average, less concern about the privacy in the model.

Experience with surveillance measure in terms of "government monitoring personal privacy" was significant, and the association was in the hypothesized direction ($b=0.03$, $t=2.15$, $p<0.10$). Controlling for the other independent variables, those having previous experience with government monitoring of personal information were more concerned about their privacy on average.

Another indicator of experience with measures, "detention resulting in search at border checkpoint" was also significantly associated with the dependent variable, and the association was in the expected direction ($b=0.84$, $t=4.57$, $p<0.01$). Controlling for other independent variables, those having previous experience of being detained at a border checkpoint were more concerned about their privacy on average.

At the bivariate analysis, three country level variables were significantly related to the privacy concern. These variables were the "democracy score", "privacy regulation", and "confidence in government". However, two of these three variables "democracy score" and "privacy regulation" were no longer significant in the multivariate model. Though another individual level independent variable -"terrorism"- was not significant at the bivariate analysis, it came up as significant.

Confidence in government was a country level variable that was significantly associated with privacy concern ($b=0.15$, $t=3.51$, $p<0.05$). All else being equal, when two countries differed in the mean citizens' confidence in government, the mean privacy concern also increased among citizens of the country with higher confidence to government on average. The results showed that when confidence increases, the privacy concerns also increases among citizens of the eight countries included in the study. This result was not in the expected direction stated in the hypothesis.

Terrorism was another country-level variable that was significantly and negatively associated with privacy concern ($b=-0.02$, $t=-3.64$, $p<0.01$). All else being equal, when two countries differed in the terrorism index, the mean privacy concern also decreased among citizens of the country the higher terrorism index. These findings will be discussed further in the next chapter.

CHAPTER V

DISCUSSION and CONCLUSION

5.1 Interpretation of Findings

The findings of the study can be summarized in three parts: First, the findings from the bivariate analysis between antecedents and privacy concerns; second, the findings from multivariate analysis with all variables; and finally, the findings on the variations of all variables across eight countries included in the study. Bivariate results showed that three of the "experience with surveillance measures" variables were significantly associated with "privacy concerns", thus demonstrating that being experienced with surveillance measures increases citizens' privacy concerns. The result supported the Smith et al.'s (1996) finding that citizens who have been exposed to measures or have been victims of personal information abuses are likely to have stronger privacy concerns.

Regarding media coverage, citizens who were more concerned about privacy were those who reported that the media pays equal attention to stories about both government violation of privacy and terrorism. Regarding the second item about media coverage the assumption was that when the media pays more attention to government violation of privacy, the citizens would have more privacy concerns. However, findings from the bivariate analysis did not support that hypothesis. This can be attributed to the difference between how much the government violation of privacy takes places in the media in reality and how people perceive the frequency of coverage. Bivariate analysis was not only conducted with individual-level, but also with country-level variables.

Examining the relationship between citizens' privacy concerns and privacy regulations, this study found a weak and negative significant relationship (r=-0.06). Studies by Milberg et al. (1995) and Zuriek et al. (2010) suggested that privacy regulations had an effect on privacy concerns. The better the privacy regulations the less the privacy concerns. The same relationship also was found for the democracy score and confidence in government variables in bivariate analysis. The privacy concern variable had a negatively weak but significant association with democracy score and confidence in government as well.

Multivariate analysis results showed that three individual-level and two country-level independent variables had statistically significant relationships with the dependent variable. However, one of the individual level variable which was knowledge of laws in public sector and one of the country level variable confidence in government were not in the hypothesized direction. The remaining variables showed that having an experience of detention resulted from a search at border check point and having an experience of prior monitoring of personal information by government increased citizens' privacy concerns. Furthermore, the country-level "impact of terrorism" variable was found to be negatively correlated with privacy concerns. These three findings were consistent with the main arguments made in the literature.

Experience with surveillance measures was a concept whose impact on privacy concern was tested by using four variables. Two of these variables of experience with surveillance were significantly associated with the dependent variable at both bivariate and multivariate analyses, which suggested a significant impact of experience with surveillance on privacy concerns. In the bivariate analysis, three out of four variables were positively

associated with privacy concerns, except for one which was “detention at airport resulting not able to board airplane”. In the multivariate analysis, two of the experience with surveillance measures variables were positively associated with citizens’ privacy concerns. This result also strengthen the findings of bivariate analysis. It can be concluded that if citizens were experienced with surveillance measures in the past, they would report more privacy concerns.

The current study also tested whether all variables at both the individual and country level, vary significantly across countries, including the dependent variable. Besides, some of the variables interestingly showed the same patterns in the country-pairwise analyses such as regulations or privacy concerns. For instance, Bonferroni correlation tables showed that there was no significant difference in terms of privacy concerns neither between the US and Canada nor between the US and China. The lack of significant difference in privacy concerns might be expected between the US and Canada, but the results that there was no difference between the US and China was surprising. Therefore, citizens’ privacy concerns should be explained by variables other than the regime type, or, in other words, the democracy score. An alternative explanations could be the technological opportunity or the power structure of the states.

Consistent with the argument of the previous paragraph that China and the US did not differ in terms of privacy concerns and showed higher level of concerns, privacy regulation (privacy index) score were the lowest in China and in the US, whereas it was the highest in Canada. The top three democracy scores among eight countries belonged to Canada, Spain and the US, whereas the lowest score belonged to China. The analysis of another country-level variable “confidence in government” pointed out that China was

interestingly the highest in confidence in government, while the US and Canada this time were in the middle of the scale.

Another country level variable was terrorism. The countries experienced terrorist attacks a short time ago naturally showed high scores in Global Terrorism Index (GTI). The first two rows consisted of Spain and the US because of Madrid train bombings in 2004, and the 9/11 attacks in 2001. It was evident that memories of citizens about those unfortunate incidents in both countries were still fresh. Their experience with terrorism might have affected their views about privacy concerns. Citizens in Spain reflected lower level privacy concerns, therefore this might be related to the recent terrorist attack, which is also consistent with multivariate regression analysis results. Moreover, the results of the chi-square test revealed that citizens of Spain reported believing that the media pays more attention to terrorism to a greater extent than any of the other countries included in the study. Again, this shows a consistency among the results despite different data sources.

Citizens' "knowledge of laws" also significantly differed across countries. The most knowledgeable citizens were Americans and followed by Canadians. These results were valid for knowledge of laws about the privacy of personal information both in public and private sectors. Citizens from Brazil and Hungary had less knowledge about laws. According to the literature, normally citizens with more knowledge of laws were expected to be more concerned about privacy. Thus, US citizens with more knowledge of laws had more concern about privacy. The third country in the row was Canada in terms of privacy concerns and second in terms of knowledge of laws. In this vein, knowledge of laws might have relative impact on citizen privacy concerns when the country scores are examined separately.

The perception that there were media coverage about safety of personal information privacy was interestingly highest in the US and then in China. This result is consistent with the higher privacy concerns of both countries. On the other hand, participants reported less media coverage on the same issue in Brazil and France.

Chinese participants reported the highest scores of that media pays more attention to government violation of privacy, and that media pays equal attention to both (terrorism and government violation of privacy). This result also reminded the highest score of confidence in government in China. When citizens report that media pays more attention to government violation of privacy, it might also be plausible to expect lower level of confidence in government. But here it is not the case. A study (Norris & Inglehart, 2007) argues that countries with censorship over the media had also showed higher scores of confidence in government. This is because citizens were not informed adequately about the policies, and people in such countries reflected higher confidence in government since they do not know the facts or they fear from the suppression of the authoritarian governments. The current study used the same data as Norris and Inglehart (2007), which was the World Value Survey 5th Wave. Their study suggested China had higher level of confidence in government. In addition, citizens of Canada reported less media attention to government violation of privacy which also reminds the relatively higher confidence in government for this country. Therefore, the results from the data about relationship between the media coverage and confidence in government were mixed.

Another focus of this dissertation was on the impact of citizens' experience with surveillance measures, which was examined by using four individual level variables. Except one of them which was about the search at border checkpoint, remaining three

variables revealed that citizens of the US were more exposed to surveillance measures than those of other countries. This result is therefore consistent with other findings about the level of privacy concerns, knowledge of laws, and privacy regulations in the US, even though some of the variables were from different data sources. These findings form the basis of and indeed strengthen the argument that the US is a "surveillance state." . In this perspective, Schneier (2014) stated that the surveillance state is politically, technically, and legally robust in the US. Moreover, he stated that the NSA does not tell the truth about its capabilities, and government surveillance is not just about NSA activities. The CIA, NRO (National Reconnaissance Office), FBI, DEA, and local police departments all conduct surveillance, and share information with each other. Taken together, the state carries out surveillance in all sectors of the life.

Schmitt (2014) advocated just the opposite view that the employees of intelligence organizations and agencies would not tolerate privacy abuses and threats to civil liberties, and they would go public to reveal the truth. Therefore, he found impossible for American intelligence community to violate the privacy of its citizens for a long time without being detected. Schmitt (2014) believes that these agencies would have more to lose and less to gain by violating laws on collecting personal information. After the two opposite views outlined above, the current study would support a middle way. Even though, the findings from the analysis supported that the US show the surveillance state features, and the real surveillance capabilities of the NSA and others are not known, it can still be said that the current system would not give way to any long lasting abuse of authority. It is particularly difficult to hide any abuses of authority in the present day, digital age. The nature of fighting crime and terrorism prohibits disclosing the capacity of security forces, but it

would be normal to expect that their capability is far beyond the current technology known to the public and also beyond the technological capacity of the private sector.

At this point the issue of harm is also important. The US Supreme Court dismissed a case in which privacy advocates sued the NSA for bulk data collection from phone companies. The case was dismissed because the Court asked about any harm inflicted (Stephens, Scheb, & Glennon, 2015). Hence, trust is the law enforcement expectation from citizens in the fight against evil. On the flip side, trust does not work every time, therefore there must be some kind of checks and balances and independent oversight mechanisms that cannot be influenced by politicians. Historically, there are many examples of abuse of power. These instances may be more limited in democratic countries, but it is evident that state surveillance capabilities have been used by governments or by leaders to repress their opponents in the past.

5.2 Discussion

Most of the time the debate on privacy and security rights raises a question about the hierarchy. Maslow's (1943) hierarchy of need theory is important in terms of determining priority among basic needs. After physiological needs, safety and security are the next most important in the hierarchy of needs pyramid. Even though privacy is not stated directly, it can be located in the third level of needs, which include belongingness and love, or in the other levels of needs that follow. Therefore, according to Maslow's hierarchy of needs, security is expected to come before the privacy. This argument can be followed by another question as to whether this priority changes over time and according to what social, economic, and political circumstances.

This study examined the impact of social and political factors, specifically experience with surveillance measures, knowledge of laws, media coverage, confidence in government, regime type, terrorism, and privacy regulations on citizens' privacy concerns. One of the findings of this study was that citizens who experience terrorist attacks in the recent past value security measures more than their privacy because of their fresh memories of the attack. Among countries in the sample, the last terrorist attack, for instance, had been experienced by the Spanish citizens with the Madrid bombings in 2004, and they showed lower concern about privacy. This might suggest that security is perceived as more of a priority than the privacy in the hierarchy of the human needs. Especially in emergency situations, public attention shifts very fast towards the personal safety and security. Even if citizens value privacy, extraordinary circumstances and events can shift their focus. Therefore, citizens can tolerate infringements to privacy because of fear and anger to some extent. Such a tolerance should not lead government agencies to ignore citizens' privacy rights. Instead, privacy intrusions by the state should be tied to legitimate and strict rules, judicial discretion, probable cause, and oversight mechanism in a democratic society to promote both privacy and security (Moore, 2011). States should carry on the fight against terrorism in democratic ways.

Moreover, it is useful to keep in mind that in some circumstances the violation of privacy (i.e., failure to keep personal information) by authorities, can increase the vulnerability to be victims of crimes. In such instances, privacy would be equal to that of safety and security. For example, if citizens' identification numbers, social security numbers, health condition information, and information about economic assets were hacked, stolen, and publicized, or were not able to be protected by data protection

authorities, then this would create both an actual and perceived insecurity. The personal information of citizens can be exploited by identity thieves, which in turn can ruin a person's life.

When people are concerned about privacy, they actually imply the fear from possible harm and from being victimized. For instance, if someone looks in through your kitchen window, although you are doing nothing suspicious to hide, you will be concerned that the person watching you from outside your kitchen window might be planning to steal something or preparing for assault. From this example, it might be inferred that privacy is also an individual safety concern and an interest in being free from harm (Brooks, 2013). This example is also to discredit the argument of "nothing to hide, nothing to fear". It provides a good reason for hanging curtains, even if you have nothing to hide. If citizens are concerned about government surveillance, they actually are concerned that government might abuse its power. Therefore, these arguments suggest that a right to privacy is related to being free from harm; that is security. Furthermore, right to privacy is related to "human security" which is the raising focus and concern of globalization.

As for the regime (democracy score) aspect, despite the fact that the democracy score of the US is high among the other the countries in the sample and China has the lowest score, these two countries do not differ in terms of privacy concerns and privacy regulations. This result strengthens the Privacy International (2014) advocacy organization's argument that today endemic surveillance may not exist only in authoritarian countries but also in democratic ones. Therefore, a regime type is not the precise indicator for privacy concerns or regulations but, rather other indicators should be considered, such as power or opportunity. Given that Eye Five countries share information

with each other, it is not surprising that the powerful countries - given that they have technological power, that communication cables pass through their territory, and that the centers of giant internet companies are located within their borders – would use this opportunity to collect big data. Hence, the fair question here would be whether another country with the same power and opportunity would do the same thing in terms of surveillance and collecting personal information.

The statistical analysis showed that the US scored almost the highest in the experience of their participants with surveillance measures. Among the citizens of eight countries, Americans reported to be the most exposed to surveillance measures. The country had also the lowest level of regulations protecting privacy, and its citizens' privacy concern was also the highest on average. In other words, American citizens reported more experience with surveillance, more privacy concerns and less quality of privacy regulations. In this vein, the US seems to need an improvement in the protection of privacy policy it has a leading role in the world as a democratic country. According to Klosek (2007), the US policies have the potential to affect countries all over the world. He also argued that the US-led war on terror affected privacy rights on global level because most of the countries enacted new laws and increased their surveillance capacities and data collection practices. If the violation of privacy, human rights, and civil liberties are experienced in the US, then the country loses its legitimacy to speak out against other governments when they commit similar violations, even against the US citizens living abroad.

5.3 Limitations

There were some limitations to this dissertation project. First of all, this dissertation used a collection of secondary datasets, and the researcher did not have a control in the data collection processes. Given the scope of the study in eight countries with around nine thousand subjects, a first-hand data collection would be extremely time and resource consuming otherwise. Secondly, the study used individual and country level variables for statistical analyses. There was enough variation for at the individual level, but the variation was low at the country level as the study was focused only on eight countries. More specifically, in all of the models focused on privacy concerns, privacy regulations are an important part and furthermore these models show a two-way relationships by considering privacy regulations as both an antecedent and an outcome. The country-level variable "privacy regulations," however, did not allow the effective measuring of that kind of relationship given that there were only eight variations in this study. Therefore, the privacy regulations variable was only used as an independent variable and as an antecedent to privacy concerns. Thirdly, the GPD survey was conducted in less than ten countries. Even though the sample size at the individual-level was more than 8,000, the country-level comparison would be better for statistical analysis if the number of countries included in the GPD survey was at least 20 or more, which was beyond the control of the researcher.

Furthermore, the available data are cross-sectional that had the measurement one point in time, and it was not possible to observe changes in privacy concerns over time. Moreover, the data were collected almost a decade ago, and it does not reflect recent and related worldwide events, such as the impact of recent terrorist attacks or revelations of individuals from the intelligence community. Lastly, the GPD and other datasets were

collected in or around the year 2006. Though this data is relatively dated, the survey and collected data is unique because it is comprehensive and uses the same questionnaire about security, surveillance, and personal information privacy issues across eight countries.

5.4 Future Research

Smith et al. (2011) argued that the relationship between antecedents and privacy concerns was understudied and tenuous. This study found some significant relationships which were pointed out. Same relationships can still be examined in further studies to strengthen the findings of this study and previously indicated tenuous relationships.

Future research should investigate whether privacy concerns change over time according to place and important events such as terrorist attacks, intelligence information leaks, and so on. In addition, more than eight countries should be included in the sample to enable more variations for the statistical analysis. The additional countries should be grouped according to similar patterns. Moreover, changes over time should be observed by replicating the study across different periods of time. Such an approach could assist in revealing if any extraordinary events shape change over time.

Cross-country research should also focus on demographic variables of citizens. Demographic variables such as nationality, age, race, income, education level, and occupation might reveal different aspects of citizens' privacy concerns.

Achieving a balance between security and civil liberties is the most desired outcome of privacy regulations. Laws play an important role. Therefore a cross-national, detailed analysis of privacy regulations is needed to create better privacy regulations and

consequently adopt and implement necessary advancements in the legal systems of countries with low privacy index scores.

Furthermore, the development and welfare level of countries should be examined to see if they have any effect on the privacy concerns of citizens. It seems that most of the privacy discussions occur in developed countries. Future research should also focus on whether citizens' privacy concerns consequently affect privacy regulations by having legislators adopt new laws.

5.5 Policy Implications

The policy implications of the study include the ways of decreasing citizens' privacy concerns by establishing a proper balance between security and civil liberties. To achieve this balance Duncan (as cited in Shane et al., 2004) discussed the tension between privacy/confidentiality and data access issues and suggested four factors as policy implications. According to the author, policy makers have to pay attention to ethical principles, democratic accountability, constitutional empowerment, individual autonomy, and information justice. To resolve the tension two effective mechanisms would be to restrict data and limit access. Appropriate policies must be responsive to changes in the realities experienced by society. Information technology and associated processes change very fast. These changes should also be reflected in policy formulation. In this regard, Cole (2014) placed an emphasis on the necessity of revising and empowering of laws that are responsive to digital age and to change in and experienced by society.

In order to strike the right balance between security and privacy, the following suggestions should also be incorporated to policy formation. First, states should develop and accept a hierarchy of values, and the risk from security threats should be proportionate

to the level of the privacy intrusion. Second, the need for personal information to be public information should be identified narrowly and stated clearly. The clear distinction would prevent the loss of citizens' privacy. Third, checks and balances should be institutionalized. This refers to the necessity of independent oversight mechanisms such as establishing a data protection agency. Such an independent institution or board can ensure that the intrusion to privacy only occurs if the threats are imminent and substantial, and that privacy is restored once the threat is diminished. Fourth, technological computerized designs can be used for controlling and preventing privacy intrusions. To this end, personal information can be processed only when the system found specific hit about a risk person rather than processing the entire identifiable data between parties for security. The architectural design of technology may be used in this case to protect the processing of personal information between allied parties in terms of security measures. The design that will be blind to database until it finds a risky personal information would be a safeguard to data processing system. The independent oversight of technological configuration would be easier than the use of specific data (Reidenberg, 2004, as cited in Shane et al. 2004).

As another policy implication, appropriate technology should be provided by private companies that enable the encryption of personal information and end-to-end communications. If people know, use, and trust these companies, they would be less concerned. In a recent example, the data encryption has been debated between the multinational technology company Apple and the FBI. After the San Bernardino shooting, which took place in December 2015 and resulted in 14 deaths and 22 injuries, the FBI recovered the cellphone of one of the perpetrators who was killed after the attack. The FBI, however, could not retrieve the stored data inside the -phone because of the previously

installed security software created by Apple. The system was designed to delete all the data stored in the phone after an incorrect password was entered 10 times. The FBI requested that Apple develop new software that can enable federal law enforcement to access encrypted data in I-phones. Apple refused to honor the FBI's request because of concerns about data privacy and the security of its customers. The FBI then brought the case to the court. However, the hearing was postponed and the FBI withdrew the case with the claim that a third party was able to break through the phone's security features and access the encrypted data. Future controversy was appeased when Apple refused to decrypt the data in the phone and the FBI withdrew its case, but it seems that the debate could arise again in the future. On the other hand, even though Apple tried to protect the data of hundreds of millions of its customers, the FBI still found a way to break the security wall and access the data they wanted. The debate showed that both parties care about the public debate and citizens' concerns. However, when data is desired by a federal law enforcement agency and it is related to a terrorism investigation, the agency will find a way to obtain the desired information (Hodson, 2016).

5.6 Conclusion

When traveling within a country or internationally, airport security measures sometimes take a long time. If we ask ourselves which option we would prefer – boarding the airplane quickly without extensive security measures or with security checks even it costs us more time, what would be the answer? Would we want to fly in an aircraft if it was found to contain explosives that successfully passed through a check point without being detected? Most of us would prefer to sacrifice some time and even some of our privacy by having our belongings checked by officials instead of boarding our flights faster

and with limited security measures. It is obvious and also supported by the study results that citizens will continue to value security more than privacy especially when memories of terrorist acts are fresh in their minds.

The public opinion polls from 2014 and early 2015 by PEW research revealed that concerns about privacy had increased. Therefore, at that time, the trend was on the privacy side. But after the recent terrorist attacks in the European metropoles of Paris and Brussels, as well as the San Bernardino, California shootings and the prevalence of fear stemming from the ISIS, the change in trends about privacy and security are possible.

Privacy concerns differ according to place, time, and culture. This study found support for place and culture in terms of different countries and confidence in government as a cultural value. Citizens' privacy concerns should be decreased by explaining the surveillance and security measures to the public. Procedural justice, transparency, accountability, and openness of laws are important in that matter. Secret laws with secret interpretations do not fulfill the qualification of being law. According to Shane et al. (2004), safety should not be equated to secrecy because it threatens not only citizens' liberty but also their security. In addition, citizens' confidence in the fair treatment of their personal information is crucial for them to have a sense of security.

Surveillance and personal data collection by both government and the private sectors should have two bases: Lawfulness and individual consent (Rule, 2007). According to Pillar (2013), citizens' are more concerned about government data collection than private sector data collection. Pillar (2013) argued that this concern is disproportionate because the private sector actually collects more personal data than the public sector does. Further, he even insisted that the NSA is more transparent than the private technology companies of

Silicon Valley. Private companies should therefore train their employees about how to protect privacy and handle personal data in such a way that is consistent with data protection principles.

Approaches that emphasize cultures of fear and lesser evil lead to harsh prevention and even preemption policies. The level of fear may vary from country to country, but with widespread media coverage on transnational terrorism, particularly with threats from the terrorist group ISIS, the public may prove to tolerate intrusive regulations to some extent.

Another point of interest related to this study is the question of why we care about citizen concerns. As discussed in the literature review chapter, there were different views about the importance of public opinion. Although public policy makers and legislators do not necessarily adopt public opinions and do not act accordingly, they still need to know what citizens think about a specific subject. Before making important decisions that may affect the majority of population, the decision makers usually need to examine public opinion trends. Regardless of whether it is adopted or not, public opinion is important in democracies. Even if they are completely supported or even supported by a majority, for their successful implementation, policies need some level of support from the public. The media has an important role to play in terms of public opinion formation and it also has the potential to be manipulated by government or decision makers. The media has an important role to play in shaping public opinion, and it is vulnerable to a manipulation of the government or decision makers.

Consequently privacy in some situations is as important as security. Security and surveillance measures should be implemented with maximum attention to liberties. There should be an impartial and independent oversight mechanism. State officials who govern

should not allow terrorists to cause significant changes to our societies and take away the liberties and freedoms that are essential to democracies. They need to at once provide both privacy and security for their citizens.

BIBLIOGRAPHY

Acquisti, A. (2004, May). Privacy in electronic commerce and the economics of immediate gratification. In M. Janssen, H. G. Sol, and R. W. Wagenaar (Eds.), *Proceedings of the 5th ACM Conference on Electronic Commerce* (pp. 21-29). doi: 10.1145/988772.988777

Alderman, E., & Kennedy, C. (1997). *The right to privacy*. New York, NY: Vintage Books.

Bøllingtoft, C. W., Vognæs, S. F., Elmquist-Clausen, C., Genest, R. L. E., Helvacı, P., & Vognæs, S. (2014). *Under the guise of national security: Surveillance, Snowden and the challenges to democracy* (Project thesis). Retrieved from: http://rudar.ruc.dk/handle/1800/13534

Baer, D., Curtis, J., Grabb, E., & Johnston, W. (1995). Respect for authority in Canada, the United States, Great Britain, and Australia. *Sociological Focus, 28*(2), 177–195.

Banisar, D. & Davies, S. (1999). Privacy and human rights 1999: An international survey of privacy laws and developments. Retrieved from Global Internet Library Campaign website: http://gilc.org/privacy/survey/

Bansal, G., Zahedi, F., & Gefen, D. (2008). The moderating influence of privacy concern On the efficacy of privacy assurance mechanisms for building trust: A multiple-context investigation. *ICIS 2008 Proceedings*, Paper 7. Retrieved from: http://aisel.aisnet.org/icis2008/7

Bansal, G., Zahedi, F., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems, 49*(2), 138-150.

Barnard-Wills, D. (2011). UK news media discourses of surveillance. *The Sociological Quarterly, 52(*4), 548-567.

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society, 20*(5), 313-324.

Betts, R. K. (2013). *Enemies of intelligence: Knowledge and power in American national Security.* New York, NY: Columbia University Press.

Beck, U. (2009). *World at risk*. New York, NY: Polity.

Bennett, C. J. (2008). *The privacy advocates*. Cambridge, MA: MIT Press.

Botello, N. A. (2010). Privacy and surveillance in Mexico and Brazil: A cross-national analysis. In E. Zureik, L. H. Stalker, E. Smith, D. Lyon, & Y. E. Chan (Eds.), *Surveillance, privacy and the globalization of personal information* (pp. 212-219). Kingston, Ontario: McGill-Queen's University Press.

Brooks, R. (2013, November 7). Privacy is red herring: The debate over NSA surveillance is about something else entirely. *Foreign Policy*. Retrieved from http://foreignpolicy.com/2013/11/07/privacy-is-a-red-herring/

Budak, J., Anić, I. D., & Rajh, E. (2013). Public attitudes towards privacy and surveillance in Croatia. *Innovation*: *The European Journal of Social Science Research*, *26*(1-2), 100-118.

Carballo, M., & Hjelmar, U. (2008). *Public opinion polling in a globalized world*. New York, NY: Springer.

Cespedes, F. V., & Smith, H. J. (1993). Database marketing: New rules for policy and practice. *Sloan Management Review*, *34*(4), 7.

Cavoukian, A. (2014). Data minding: A response to "Privacy Pragmatism". *Foreign Affairs*, *93*(5), 175-176.

Cavoukian, A. & El Emam, K. (2013). Introducing privacy-protective surveillance: Achieving privacy and effective counter-terrorism. Beaconsfield, Quebec: Canadian Electronic Library. Retrieved from https://www.ipc.on.ca/images/Resources/pps.pdf

Ceyhan, A. (2010). Privacy in France in the age of information and security technologies. In E. Zureik, L. H. Stalker, E. Smith, D. Lyon, & Y. E. Chan (Eds.), *Surveillance, privacy and the globalization of personal information* (pp.171-188). Kingston, Ontario: McGill-Queen's University Press.

Clarke, D. A. Jr. (2013). *Making U.S. security and privacy rights compatible*. (Thesis). Naval Postgraduate School. Retrieved from http://hdl.handle.net/10945/37603

Clarke, R. (2006, July). What's privacy? In Proc. of the Workshop at the Australian Law Reform Commission.

Chesterman S., (2010). Privacy and surveillance in the age of terror. *Survival: Global Politics and Strategy*, *52*(5), 31-46, DOI: 10.1080/00396338.2010.522094

Diamond, J. (2015, May 30). Patriot Act provisions have expired: What's now? CNN Politics. Retrieved from http://www.cnn.com/2015/05/30/politics/what-happens-if-the-patriot-act-provisions-expire/

Cockfield, A. J., (2010a). Legal constrains in transferring personal information across borders: A comparative analysis of PIPEDA and foreign privacy laws. In E. Zureik, L. H. Stalker, E. Smith, D. Lyon, & Y. E. Chan (Eds.), *Surveillance, privacy and the globalization of personal information*. Kingston, Ontario: McGill-Queen's University Press.

Cockfield, A. J. (2010b). Individual autonomy, law, and technology: Should soft determinism guide legal analysis?. *Bulletin of Science, Technology & Society, 30*(1), 4-8.

Cole, D. (2014, January 27). We need privacy laws for the digital era. *Nation*.

Comey, J. (2014). Going dark: Are technology, privacy, and public safety on a collision course? The Brookings Institution event. Retrieved from http://www.brookings.edu/events/2014/10/16-going-dark-technology-privacy-comey-fbi on 16 October 2014.

Culnan, M. J. (1995). Consumer awareness of name removal procedures: Implications for direct marketing. *Journal of Direct Marketing*, 9(2), 10-19.

Davis, D. W., & Silver, B. D. (2004). Civil liberties vs. security: Public opinion in the context of the terrorist attacks on America. *American Journal of Political Science, 48(1)*, 28-46.

De Rosa, M. (2003). Privacy in the age of terror. *Washington Quarterly, 26*(3), 27-41.

Dinev, T., Bellotto, M., Hart, P., Colautti, C., Russo, V. & Serra, I. (2005). Internet users' privacy concerns and attitudes towards government surveillance - An exploratory study of cross-cultural differences between Italy and the United States, Proceedings of the 18th Bled eConference: *eIntegration in Action*, 6-8 June, Bled, Slovenia.

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents-measurement validity and a regression model. *Behaviour & Information Technology, 23*(6), 413-422.

Dinev, T., & Hart, P. (2006). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce, 10*(2), 7-29.

Ebenger, T. (2008). The USA PATRIOT Act: Implications for private e-mail. *Journal of Information Technology & Politics, 4*(4), 47-64.

Echebarria-Echabe, A., & Fernández-Guede, E. (2006). Effects of terrorism on attitudes and ideological orientation. *European Journal of Social Psychology, 36*(2), 259-265.

ECJ, European Court of Justice. (2014). The Court of Justice declares the Data Retention Directive to be invalid. Press Release No 54/14. Retrieved from http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

EU Directive 95/46/EC - The Data Protection Directive Retrieved from http://www.dataprotection.ie/docs/EU-Directive-95-46-EC-Chapter-1/92.htm

Ferguson, S. D. (2000*). Researching the public opinion environment: Theories and Methods*. Thousand Oaks, CA: Sage Publications.

Ferguson, Y. H., & Mansbach, R. W. (2012). *Globalization: The return of borders to a borderless world*. Abingdon, VA: Routledge.

Fiss, O. (2012). Even in a time of terror. *Yale Law & Policy Review, 31*(1), 1-31.

Fournier, F. (2010). Quebec, the rest of Canada, and the international survey: A case of two solitudes? A comparative analysis of perceptions about privacy and personal information issues. In E. Zureik, L. H. Stalker, E. Smith, D. Lyon, & Y. E. Chan (Eds.), *Surveillance, privacy and the globalization of personal information* (pp. 127-146). Kingston, Ontario: McGill-Queen's University Press.

Fox, J. (1991). *Regression diagnostics: An introduction* (Vol. 79). Newbury Park, CA: Sage Publicaitons Inc.

Fura, E., & Klamberg, M (2012). The chilling effect of counter-terrorism measures: A comparative analysis of electronic surveillance laws in Europe and the USA. In J. Cassadwell, E. Myjer, & M. O'Boyle (Eds.), *Freedom of expression-Essays in honor of Nicolas Bratza-president of the European Court of Human Rights* (pp.463-481). Oisterwijk: Wolf Legal Publishers.

Furedi, F. (2006). *Culture of fear revisited*. London, UK: Bloomsbury Publishing.

Gandy, O. H. (2003). Public opinion surveys and the formation of privacy policy. *Journal of Social Issues, 59*(2), 283-299.

Garfinkel, S. (2000). *Database nation: The death of privacy in the 21st century*. Sebastopol, CA: O'Reilly Media, Inc.

Gerbner, G. (1998). Cultivation analysis: An overview. *Mass Communication and Society, 1*(3-4), 175-194.

Grenville, A. (2010). Shunning surveillance or welcoming the watcher? Exploring how people traverse the path of resistance. In E. Zureik, L. H. Stalker, E. Smith, D. Lyon, & Y. E. Chan (Eds.), *Surveillance, privacy and the globalization of personal information* (pp. 70-83). Kingston, Ontario: McGill-Queen's

University Press.

Goold, B. J. (2010). How much surveillance is too much? Some thoughts on surveillance, democracy, and the political value of privacy. In D. W. Schartum (Ed.), *Overvåkning I En Rettsstat – Surveillance in a constitutional government* (pp 38-48). Bergen: Fagbokforlaget. http://ssrn.com/abstract=1876069

GPD Project (2014). Privacy and Surveillance: February/March 2014 Globalization of Personal Data follow-up study conducted by the Vision Critical division of the polling company Angus Reid Global Retrieved from http://qspace.library.queensu.ca/handle/1974/12285

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the US surveillance state*. New York, NY: Metropolitan Books.

Hallinan, D., Friedewald, M., & McCarthy, P. (2012). Citizens' perceptions of data protection and privacy in Europe. *Computer Law & Security Review*, *28*(3), 263-272.

Haggerty, K. D. & Ericson, R. V. (Eds.). (2006). *The new politics of surveillance and visibility*. Toronto: University of Toronto Press.

Haggerty, K. D., & Gazso, A. (2005). Seeing beyond the ruins: Surveillance as a response to terrorist threats. *Canadian Journal of Sociology/Cahiers Canadiens de Sociologie*, *30*(2), 169-187.

Harris, L. & Westin, A. F. (Ed.). (1991). *Harris-Equifax consumer privacy survey 1991*. Atlanta, GA: Equifax Inc.

Hetherington, M. J., & Nugent, J. D. (2001). Explaining public support for devolution: The role of political trust. In J. R. Hibbing & E. Theiss-Morse (Eds.), *What is it about government that Americans dislike* (pp. 134-151). Cambridge, UK: Cambridge University Press.

Hodson, H. (2016). Apple vs FBI: First salvo in the information war. *New Scientist, 229*(3062), 24-25.

Hofstede, G., Hofstede, G. J., & Minkov, M. (1991). *Cultures and organisations-software of the mind: Intercultural cooperation and its importance for survival*. New York, NY: McGraw-Hill.

Hofstede, G. (2001). *Culture's Consequences: Comparing values, behaviors, institutions, and organizations across nations*. Thousand Oaks, CA: Sage Publications.

Hofstede, G. (2014). National culture. Geert-Hofstede Web-Site. Retrieved from http://geert-hofstede.com/national-culture.html

Hough, P. (2008). *Understanding global security*. New York, NY: Routledge.

Institute for Economics and Peace, IEP. (2006). Vision of humanity. Terrorism Index 2006 global rankings. Retrieved from http://www.visionofhumanity.org/#page/indexes/terrorism-index/2006 on 12 February 2015.

Institute for Economics and Peace, IEP. (2014). Vision of humanity. Measuring and understanding the impact of terrorism. Global Terrorism Index. Retrieved from http://www.visionofhumanity.org/sites/default/files/Global%20Terrorism%20Index%20Report%202014_0.pdf

Ignatieff, M. (2004). *The lesser evil: Political ethics in an age of terror*. Princeton, NJ: Princeton University Press.

Inglehart, R., & Welzel, C. (2004). What insights can multi-country surveys provide about people and societies? *American Political Science Association-Comparative Politics Newsletter, 15*, 6-11.

Ipsos Reid (2006). The Globalization of Personal Data (GPD) Project, International Survey on Privacy and Surveillance. Data file retrieved from http://hdl.handle.net/1974/7753.

Kekic, L. (2007). The Economist Intelligence Unit's index of democracy. *The Economist*, *21*, 1-11.

Kerr, O. S. (2003). Internet surveillance law after the USA Patriot Act: The Big Brother that isn't. *Northwestern University Law Review, 97*(2), 607-673.

Klosek, J. (2007). *The war on privacy*. New York, NY: Greenwood Publishing.

Kossowska, M., Trejtowicz, M., de Lemus, S., Bukowski, M., Van Hiel, A., & Goodwin, R. (2011). Relationships between right-wing authoritarianism, terrorism threat, and attitudes towards restrictions of civil rights: A comparison among four European countries. *British Journal of Psychology*, *102*(2), 245-259.

Langer, G. (2002). Trust in government: To do what. *Public Perspective*, *13*(4), 7-10.

Langhorne, R. (2001). *The coming of globalization: Its evolution and contemporary consequences*. New York, NY: Palgrave Macmillan.

Lipset, S. M. (1996). *American exceptionalism: A double-edged sword*. New York, NY: W.W. Norton & Company, Inc.

Little, R. J. (1988). Missing-data adjustments in large surveys. *Journal of Business & Economic Statistics, 6*(3), 287-296.

Lyon, D. (Ed.). (2003). *Surveillance as social sorting: Privacy, risk, and digital discrimination*. New York, NY: Routlege.

Lyon, D. (2007). *Surveillance studies: An overview*. New York, NY: Polity.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15(4),* 336-355.

Margulies, P. (2014). The NSA in global perspective: Surveillance, human rights, and international counterterrorism. *Fordham Law Review, 82(5),* 2137.

Margulis, S. T., Pope, J. A., & Lowen, A. (2010). The Harris-Westin index of general concern about privacy: An exploratory conceptual replication. In E. Zureik, L. H. Stalker, E. Smith, D. Lyon, & Y. E. Chan (Eds.), *Surveillance, privacy and the globalization of personal information* (pp. 91-109). Kingston, Ontario: McGill-Queen's University Press.

Marmura, S. (2010). Security vs privacy: Media messages, state policies, and American public trust in government. In E. Zureik, L. H. Stalker, E. Smith, D. Lyon, & Y. E. Chan (Eds.), *Surveillance, privacy and the globalization of personal information* (pp. 110-126). Kingston, Ontario: McGill-Queen's University Press.

Martin, S., & Rabina, D. (2009). National security, individual privacy and public access to government-held information: The need for changing perspectives in a global environment. *Information & Communications Technology Law, 18*(1), 13-18.

Maslow, A. H. (1943). A theory of human motivation. *Psychological Review*, *50*(4), 370.

McCahill, M., & Finn, R. (2010). The Social impact of Surveillance in Three UK Schools: Angels, Devils and Teen Mums. *Surveillance & Society, 7*(3/4), 273-289.

Merino, N. (Ed.). (2015). *Privacy*. Farmington Hills, MI: Greenhaven Press.

Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. (1995). Values, personal information privacy, and regulatory approaches. *Communications of the ACM, 38*(12), 65-74.

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization Science, 11*(1), 35-57.

Moore, A. D. (2011). Privacy, security, and government surveillance: WikiLeaks and the new accountability. *Public Affairs Quarterly, 25*(2), 141-156.

Nakhaie, R., & de Lint, W. (2013). Trust and support for surveillance policies in Canadian and American opinion. *International Criminal Justice Review*, 23(2), 149-169.

Neuman, W. R., Just, M. R., & Crigler, A. N. (1992). *Common knowledge: News and the construction of political meaning*. Chicago, IL: University of Chicago Press.

Newport, F. (2013). Americans disapprove of government surveillance programs. Retrieved from http://www.gallup.com/poll/163043/americans-disapprove-government-surveillance-programs.aspx

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford University Press.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41(1),* 100-126.

Norris, P., & Inglehart, R. (2008). Silencing dissent: The impact of restrictive media environments on regime support. Midwest Political Science Association, 66th Annual Meeting (2008), Chicago, IL: American Political Science Association.

Nyst, C. (2014, July 16). UN privacy report: A game changer in fighting unlawful surveillance. Retrieved from https://www.privacyinternational.org/node/321

Page, S. (2014, January 20). Poll: Most Americans now oppose the NSA Program. *USA Today*. Retrieved from http://www.usatoday.com/story/news/politics/2014/01/20/poll-nsa surveillance/4638551/

Office of the United Nations High Commissioner for Human Rights [OHCHR] (2015). The United Nations Human Rights Treaty System: An introduction to the core human rights treaties and the treaty bodies. Retrieved from http://www.ohchr.org/Documents/Publications/FactSheet30en.pdf

Office of the United Nations High Commissioner for Human Rights [OHCHR] (2015). The Right to Privacy in the Digital Age Report. Retrieved from http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf on 7 October 2014.

PEW Research Center (2013, June 6-9). Majority views NSA phone tracking as

acceptable anti-terror tactic. Survey results retrieved from http://www.people-press.org/2013/06/10/majority-views-nsa-phone-tracking-as-acceptable-anti-terror-tactic/

PEW Research Center (2013, July 26). Government Surveillance: A Question Wording Experiment. Retrieved from http://www.people-press.org/2013/07/26/government-surveillance-a-question-wording-experiment/

PEW Research Center (2014, July 14). Global Opinions of U.S. Surveillance. Global Attitudes Project. Retrieved from http://www.pewglobal.org/2014/07/14/nsa-opinion/

Pillar. P. (2013, December 10). Big data, public and private. *The National Interest*. 12-18.

PoKempner, D. (2014, February 17). Privacy in the age of surveillance. A strong global right to electronic privacy demands recognition, in U.S. law and internationally. *Foreign Policy in Focus*. Retrieved from http://fpif.org/privacy-age-surveillance/

Privacy International (2011). European Privacy and Human Right Report-EPHR. Retrieved from http://cmds.ceu.edu/article/2014-03-09/european-privacy-and-human-rights-2010.

Privacy International (2014). Essays and blogs retrieved from www.privacyinternational.org

Privacy International (2014). International Privacy Rankings 2007. Retrieved from https://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559597 Accessed on 23 October 2014. Available on http://observatoriodeseguranca.org/files/phrcomp_sort.pdf

Poitras, L. (2015). Citizenfour. Documentary movie. United States: HBO Broadcasting.

Putnam, R. D. (2000). *Bowling alone: The collapse and revival of American community*. New York, NY: Simon & Schuster.

Rainie, L. & Madden, M. (2015, March 16). American's privacy strategies post-Snowden. Pew Research Center.

Regan, P. M. (1995). *Legislating privacy: Technology, social values, and public policy*. Chapel Hill, NC: University of North Carolina Press.

Richards, N. M. (2013). The dangers of surveillance. *Harvard Law Review, 126*(7), 1934-1965

Rosen, J. (2005). *The naked crowd: Reclaiming security and freedom in an anxious age*. New York, NY: Random House Inc.

Rule, J. B. (2007). *Privacy in peril: How we are sacrificing a fundamental right in for security and convenience*. New York, NY: Oxford University Press.

Sarat, A. (2015). *A world without privacy. What law can and should do?* New York, NY: Cambridge University Press.

Schmitt, G. (2014, February 3). Privacy or security: A false choice. *Weekly Standard*, 19.

Schneier, B. (2014, January 6). How the NSA threatens national security. *The Atlantic*, 1.

Schwartz, B. (1968). The social psychology of privacy. *American Journal of Sociology, 73*, 741-752.

Schwartz, P. M. (2008). Reviving telecommunications surveillance law. *The University of Chicago Law Review, 75*(1), 287-315.

Shane, P. M., Podesta, J., Leone, R.C. (2004). *A little knowledge: Privacy, security and public information after September 11*. New York, NY: The Century Foundation Press.

Shane, S. (2010, August 29). An arms suspect, bargaining with secrets. *The New York Times*, Retrieved from http://www.nytimes.com/2010/08/30/world/30bout.html?_r=0

Sheehan, K. B. & Hoy, M. G. (1999). Flaming, complaining, abstaining: How online users respond to privacy concerns. *Journal of Advertising, 28*(3), 37-51.

Shipler, D. K. (2011). *The rights of the people: How our search for safety invades our liberties*. New York, NY: Vintage Books-Alfred A. Knopf Publication.

Smith, H. J. (2004). Information privacy and its management. *MIS Quarterly Executive, 3*(4), pp. 201-213.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989-1016.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167-196.

Slobogin, C. (2007). *Privacy at risk: The new government surveillance and the Fourth Amendment.* Chicago, IL: University of Chicago Press.

Soghoian, C. (2012). *The spies we trust: Third party service providers and law enforcement surveillance* (Doctoral dissertation). Retrieved from Indiana University Database http://files.dubfire.net/csoghoian-dissertation-final-8-1-2012.pdf

Soma, J. T., Nichols, M. M., Rynerson, S. D., & Maish, L. A. (2004). Balance of privacy vs. security: A historical perspective of the USA Patriot Act. *Rutgers Computer & Technology Law Journal, 31*(2), 285.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477-564.

Solove, D. J. (2007). 'I've got nothing to hide' and other misunderstandings of privacy. *San Diego Law Review, 44*(4), 745-772.

Solove, D. J. (2008). *Understanding Privacy*. Cambridge, MA: Harvard University Press.

Solove, D. J. (2011). *Nothing to hide: The false tradeoff between privacy and security.* New Haven, CT: Yale University Press.

Soroka, S. N., & Wlezien, C. (2009). *Degrees of democracy: Politics, public opinion, and policy.* Cambridge, UK: Cambridge University Press.

Stephens, O. H., Scheb, J.M., and Glennon, C. (2015). *American constitutional law volume I: Sources of Power and Restraint*. Stamford, CT: Cengage Learning.

Szekely, I. (2010). Changing attitudes in a changing society? Information privacy in Hungary 1989–2006. In E. Zureik, L. H. Stalker, E. Smith, D. Lyon, & Y. E. Chan (Eds.), *Surveillance, privacy and the globalization of personal information* (pp. 150-170). Kingston, Ontario: McGill-Queen's University Press.

Taylor, N. (2014). To find the needle do you need the whole haystack? Global surveillance and principled regulation. *The International Journal of Human Rights, 18(1),* 45-67.

Taylor Jr, S. (2014). *The big snoop: Life, liberty, and the pursuit of terrorists*. Washington, DC: Brookings Institution Press.

Thesslin, G. (2011). *Being private in the surveillance society: The concept of privacy in the age of terror, CCTV, and electronic surveillance*. (Master Thesis). Universitetet i Tromsø. Retrieved from http://hdl.handle.net/10037/3511

The Surveillance Project International Survey Findings (2008). Retrieved from http://qspace.library.queensu.ca/bitstream/1974/7660/1/2008_Surveillance_Project_International_Survey_Findings_Summary.pdf

Tilly, C. (2004). Trust and rule. *Theory and Society, 33(1),* 1-30.

Warren, S. D. & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 93-220.

Webb, M. (2007). *Illusions of security: Global surveillance and democracy in the post-9/11 world*. San Francisco, CA: City Lights Books.

Weissberg, R. (2001). Why policymakers should ignore public opinion polls. *Cato Institute Policy Analysis, 402*.Retrieved from http://www.cato.org/publications/policy-analysis/why-policymakers-should-ignore-public-opinion-polls

Westin, A. F. (1967). *Privacy and freedom*. New York, NY: Athenum.

Wolfendale, J. (2006). Terrorism, security, and the threat of counterterrorism. *Studies in Conflict & Terrorism, 29*(7), 753-770.

World Walues Survey (2009). WVS database 5th wave conducted between 2005 and 2009. Retrieved from http://www.worldvaluessurvey.org/WVSDocumentationWV5.jsp

Wraight, C. D. (2009). *Rousseau's 'The social contract': A reader's guide*. London, UK: Bloomsbury Publishing.

Wirtz, J., Lwin, M. O., & Williams, J. D. (2007). Causes and consequences of consumer online privacy concern. *International Journal of Service Industry Management, 18*(4), 326-348.

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. International Conference on Information Systems 2008 Proceedings. Paper 6.

Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. (2010). The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems, 26*(3), 135-174.

Ybarra, L. (2011). EU Model as an adoptable approach for US privacy laws: A comparative analysis of data collection laws in the United Kingdom, Germany, and the United States. *Loyola Los Angeles International & Comparative Law Rev*iew, *34*(2/4), 267.

Zureik E. (2004). Governance, security and technology: The case of biometrics. *Studies of Political Economy (73),* 113-137.

Zureik, E. & Stalker, L. H. (2010). The cross-cultural study of privacy. In E. Zureik, L. H. Stalker, E. Smith, D. Lyon, & Y. E. Chan (Eds.), *Surveillance, privacy and the globalization of personal information* (pp. 5-27). Kingston, Ontario: McGill-Queen's University Press.

Zureik, E., Stalker, L. H., Smith, E., Lyon, D., & Chan, E.Y. (Eds.). (2010). *Surveillance, privacy and the globalization of personal information*. Kingston, Ontario: McGill-Queen's University Press. 2010). Chan (Eds.), *Surveillance, privacy and the globalization of personal information* Kingston, Ontario: McGill- Queen's University Press.

APPENDIX

List of Privacy Advocacy Organizations

Organization	*Abbreviation*	*Country*
Alfa-Redi		Peru
American Civil Liberties Union	ACLU	United States
Amnesty International	AI	International
Arbeitskreis Vorratsdatenspeicherung (Working Group on Data Retention)		Germany
Arge Daten Austria Association Electronique Libre (Electronic Freedom Association)	AEL	Belgium
Association for Technology and Internet	APTI	Romania
Australian Privacy Foundation	APF	Australia
Bits of Freedom	BoF	Netherlands
British Columbia Civil Liberties Association	BCCLA	Canada
Buro Jansen and Janssen		Netherlands
Californians against Telephone Solicitations	CATS	United States
Campaign for Digital Rights	CDR	United Kingdom
Canadian Civil Liberties Association	CCLA	Canada
Canadian Internet Public Policy Clinic	CIPPIC	Canada
CATO Institute	CATO	United States
Center for Digital Democracy	CDD	United States
Center for Democracy and Technology	CDT	United States
Chaos Computer Club	CCC	Germany
Coalition Against Unsolicited Commercial Email	CAUCE	United States
Computer Professionals for Social Responsibility	CPSR	United States (Chapters in Canada, Spain, Peru, Africa, Japan)

Organization	*Abbreviation*	*Country*
Consumer Action	CA	United States
Consumer Association		United Kingdom
Consumers Against Supermarket Privacy Invasion and Numbering	CASPIAN	United States
Cyber-Rights and Cyber-Liberties		United Kingdom
Derechos Digitales (Digital Rights)		Chile
Deutsche Vereinigung fu¨ r Datenschutz (German Association for Data Protection)	DVD	Germany
Die Humanistische Union (The Humanist Union)	HU	Germany
Digital Rights Denmark		Denmark
Digital Rights Ireland		Ireland
Electronic Frontier Finland	EFFI	Finland
Electronic Frontier Foundation	EFF	United States
Electronic Privacy Information Center	EPIC	United States
European Civil Liberties Network	ECLN	Europe
European Digital Rights Initiative	EDRI	Europe
FoeBuD		Germany
Fo¨rderverein Informationstechnik und Gesellschaft (Association for Information Technology and Society)	FITUG	Germany
Forum Informatikerinnen fu¨ r Frieden and gesellschaftliche Verandwortung (Forum of Computer Professionals for Peace and Social Responsibility)	FIFF	Germany
Foundation for Information Policy Research	FIPR	United Kingdom
Foundation for Taxpayer and Consumer Rights	FTCR	United States

Organization	*Abbreviation*	*Country*
Frontline		Canada
Fundacion via Libre (Open Source Foundation)		Argentina
Global Internet Liberty Campaign	GILC	International
Health Privacy	HP	United States
ID Theft Resource Center	ITRC	United States
Imaginons un Re´seau Internet Solidaire	IRIS	France
International Civil Liberties Monitoring Group	ICLMG	Canada
Internet Society		Bulgaria
Iuridicum Remedium		Czech Republic
Junkbusters		United States
La Ligue des Droits et Liberte´s (League of Rights and Liberties)		Quebec, Canada
Leave Those Kids Alone	LTKA	United Kingdom
Liberty Coalition		United States
Medical Privacy Coalition	MPC	United States
Motorists Against Detection	MAD	United Kingdom
National Association of State Public Interest Research Groups	US PIRG	United States
National Consumers League	NCL	United States
National Council for Civil Liberties	NCCL	United Kingdom
Netjus		Italy
Netzwerk Neue Medien (Network New Media)	NNM	Germany
New York Surveillance Camera Players	SCP	United States
NO2ID		United Kingdom
Patient Privacy Rights Coalition		United States
Privacy International	PI	United Kingdom

Organization	*Abbreviation*	*Country*
Privacy Rights Clearinghouse	PRC	United States
Privacy Ukraine		Ukraine
Privacy Activism		United States
Privacy Journal		United States
Privacy Mongolia		Mongolia
Privacy Times		United States
Private Citizen, Inc.		United States
Privaterra		Canada
Public Interest Advocacy Center	PIAC	Canada
Public Interest Computing Association	PICA	United States
Quintessenz		Austria
Seguridad en Democracia (Security and Democracy)	SEDEM	Guatemala
Statewatch Europe		
Stichtung Waakzaamheid Persoonregistratiie (Privacy Alert)		Netherlands
Swiss Internet User Group	SIUG	Switzerland
Transatlantic Consumer Dialogue	TCD	Europe
UK National Consumer Council	NCC	United Kingdom
Utilities Commission Action Network	UCAN	United States
Verbraucherzentrale Bundesverband (Federation of German Consumer Organizations)	VBV	Germany
Verein fu¨ r Internet-Benutzer O¨ sterreichs (Association for Austrian Internet Users)	Vibe AT!	Austria
World Privacy Forum	WPF	United States