Your Data Shadow:

An exploratory study of the short-term effect of viewing news and information content on surveillance technologies on perceptions of privacy

by

Natalie Farid

A thesis submitted to the Faculty of Graduate and Postdoctoral Affairs in partial fulfillment of the requirements for the degree of

Master of Arts

in

Legal Studies

Carleton University

Ottawa, Ontario

Abstract

This exploratory study measures the effect of viewing news stories and information about privacy breaches and surveillance technology, on awareness and sensitivity to privacy and the protection of personal information. There has been little empirical examination of the effect of surveillance awareness despite a growing body of scholarship devoted to theorizing surveillance and privacy. Participants in an experimental group (N=30), comprised of Carleton University students were exposed to a series of short documentary and news stories (26 minutes) about breaches in privacy and asked to respond to written questions about their perceptions relating to privacy awareness, vulnerability and prevention. These responses were compared to a control group (N=30). The findings suggest that knowledge about surveillance technologies such as biometrics and privacy are limited among all participants. The experimental group however, demonstrated elevated concerns about their privacy after being exposed to the video; thus demonstrating educational programming's powerful immediate effect.

Acknowledgements

Thank you very much Lord for your love, comfort; for being my strength and guide in the writing of this thesis.

I am profoundly thankful to my supervisor Professor George S. Rigakos for his selfless dedication to both my personal and academic development. I am tremendously grateful for his support, guidance, comments, thorough and excellent feedback and engagement through the process of this master thesis. It has been an honour to work under his direction and having been a student in his classes. I am very fortunate to have had him as my supervisor. His incredible wealth of knowledge and professional accomplishments are inspiring.

My dear mother Magda and brother David, I am grateful to have you as my loving family; you have both been tremendously encouraging throughout this entire process. I would also like to express my gratitude towards Francesca and my wonderful friends who always believed in my aspirations and provided constructive criticism. I am immeasurably blessed to have you all in my life.

Thank you to all the participants who took part in my research study, who have willingly dedicated their precious time and energy.

Finally, I would like to acknowledge and thank the Faculty of Graduate and Postdoctoral Affairs for awarding me with a research bursary which allowed me to advance in this research.

"Learning is not attained by chance, it must be sought for with ardor and attended to with diligence." – Abigail Adams

Table of Contents

Chapter One: Introduction

It might seem that despite increasing advancements in surveillance technology, Canadians are not significantly concerned about privacy. When you make a simple purchase, for instance, at a furniture store, the store cashier may request personal information such as your home address and telephone number. Many of us voluntarily provide this personal information without much hesitation, but are we aware of why an institution is collecting our personal information, and if so, have we really considered the consequences arising from providing it? Between 2003 and 2007, more than 20 million credit and debit card numbers were stolen by hackers from TJX Co. (Pilieci 2010). In June 2010, Google surreptitiously collected private Wi-Fi data in 30 countries (Pilieci 2010). According to Ontario's information and privacy commissioner, Ann Cavoukian, the world has less than a decade to make the protection of personal information and online privacy a priority, before these concepts cease to exist (Pilieci 2010). The main objective of this exploratory study is to empirically test the effect of viewing news content about breaches of privacy. In particular, whether exposure to such news affects awareness or potential precautionary behaviour. Such research is crucial, as the findings can contribute to future planning, i.e., with regards to the creation of privacy laws in Canada, as well as the manner in which technology devices are developed and implemented. If a particular group of people (e.g., students), do not have a serious regard for privacy, this lack of awareness may mitigate against their protecting personal information to reduce potential risks, such as fraud, identity theft, profiling, and so forth.

The central research question guiding this thesis concerns the impact of surveillance technologies on the perceived privacy of individuals in Canada, and whether creating awareness of the consequences of such breaches in privacy causes people to perceive it differently. How does increased awareness of surveillance technology and its range of actual and potential uses affect people's concerns about privacy? Does viewing material about breaches in privacy affect attitudes toward social media, RFID and so forth? More specifically: How do individuals regard and understand the notion of privacy? How do people respond or react to particular surveillance technologies (e.g., closed circuit television surveillance, Facebook, biometric software, radio-frequency identification tags, etc.)? Furthermore, are individuals aware of the manner in which surveillance technologies are used?

Public Awareness

Public opinion research in Canada consistently shows strong support for the use of camera surveillance in public and in private spaces while scholarly studies report significantly lower acceptance, and focus group findings show an ambivalence towards surveillance cameras. (Deisman & Derby, 2009). A public opinion poll reveals that most people in Norway are fairly supportive of CCTV (Closed Circuit Television) (Saetnan & Dahl 2004, 38). In addition, in Canada, public opinion polling indicates a high level of general acceptance of national ID cards (approximately two-thirds) (Lyon 2003). Polls conducted in Australia overwhelmingly indicate that the public's main concern with respect to privacy invasion, is the proliferation and cross-matching of databases (Australian Press Council 2004).

A comparative research study of surveillance and privacy was conducted, and the findings from a survey administered in Canada and the United States in 2006, which was repeated in a 2012 poll, indicate some continuities and relevant changes in attitude, overtime. Knowledge of the internet and software such as GPS (Global Positioning System) is relatively high in both countries and is higher among younger groups, especially males. Similarly, a higher proportion than previously, now think they have a say over what happens to their personal data – the younger, the more so. In both Canada and the United States, more people than before believe that camera surveillance is effective. However, a greater proportion now consider security-surveillance intrusive. Individuals take precautions to protect their personal data in both countries (i.e., Canada and the USA), although they are much more concerned about what corporations may do with their information (Smith & Lyon 2013, 190). In addition, differences in age and gender are also linked to variations in precautionary behaviour (Smith & Lyon 2013, 190). In 2006, Zureik led a nine-country international survey on attitudes about surveillance and privacy, and experiences with the global flow of personal data. Telephone, face-to-face and online interviews were conducted with 9,606 respondents in Canada, the USA, Brazil, Mexico, China, Japan, France, Hungary and Spain. The survey included 50 questions on participants' attitudes about consumer surveillance, racial profiling, national ID cards, CCTV, media coverage of surveillance issues, knowledge of various technologies, actions taken to protect information and control over personal data (Zureik 2010). In 2012, a follow-up survey contained 10 of the original survey questions from 2006, and 14 additional questions about new technologies, with a focus on social media in particular. The sampling techniques for the 2006 and 2012 surveys differ

greatly. As this research is the most comprehensive to date, it is worth closer scrutiny (Smith & Lyon 2013, 192).

Knowledge about GPS increased in both countries, with about 10% in reported knowledge (from 55 to 64 per cent in Canada, and 60 to 70 per cent in the US), from 2006 to 2012. In contrast, knowledge about RFID, CCTV, biometrics and data mining decreased since 2006. The 2006 and 2012 findings reveal a decline in reported knowledge of these surveillance technologies in older age groups; CCTV being the exception – slightly higher in the 55+ category in 2012. More men than women reported being knowledgeable about all of the aforementioned technologies – in 2012: GPS- 71% and 55%, RFID- 36% and 14%, CCTV- 58% and 36%, Biometrics- 31% and 17%, Data mining- 36% and 17%. (Smith & Lyon 2013, 192). Younger respondents between the age of 18 to 34 years, in both surveys felt they had more control over what happens to their personal information than older respondents (35 to 54 years of age). In 2006, 39% of the younger people felt they had more say in what happens to their personal information, whereas only 27% of the older people believed the same. In 2012, 51% of the younger generation felt they had more say, versus 44% of the older generation. (Smith & Lyon 2013, 193). In 2012, Canadians (56%) felt they were doing well at protecting their own personal information. Compared with the Office of the Privacy Commissioner (OPC) findings from 2006, Canadians have become more confident that businesses are taking their responsibility seriously, in protecting consumers' personal information (14%), 13% disagreed and 68% believe businesses were taking it somewhat seriously. Regarding community CCTV effectiveness, there is an increase (from 79 to 87%), in Canada. (Smith & Lyon 2013, 195-196).

In comparing 2006 to 2012 findings, respondents remained reticent about sharing information with companies and less so with government. The most notable increase occurred with respondents purposefully giving false information about themselves to marketers (from 20 per cent to 43 per cent in Canada and from 22 to 35 per cent in the US); thus, suggesting a greater awareness of the need to protect personal information, which is demanded at every consumer transaction. (Smith & Lyon 2013, 199-200). In 2012, the older the age category, the more likely respondents were to refuse providing information to a business because they thought it was not necessary. However, younger people were more likely to purposely give incorrect information to marketers – 46% of 18 to 34 year olds – compared to 39% of 35 to 54 year olds. Differences in terms of gender were minimal – more men (44%) than women (38%), purposely providing incorrect information when using the internet. (Smith & Lyon 2013, 201).

The Office of the Privacy Commissioner found that 65% agreed that protecting Canadians' personal information will be one of the most important issues facing the country in the next 10 years, and 60% believed they had less protection over their personal information in their daily lives, than they did 10 years ago. (OPC 2011).

Smith and Lyon point out that gender differences in use of technology, and experiencing surveillance, combined with age are an area of research needing further exploration. In addition, reasons for variation in opinion between surveillance domains, is also an area which requires more research. However, most importantly, subjectivity and how individuals experience surveillance in all aspects of their lives needs to be sought through various methods, in order to reveal the complex picture of how individuals

accept, negotiate, comply with, reject, ignore, are unaware of, engage with or participate in the surveillance which permeates their lives. (Smith & Lyon 2011, 201-202).

According to a 2011 study conducted by the federal Office of the Privacy Commissioner, approximately 6 in 10 Canadians felt that they had less protection of their personal information in their daily lives than they did a decade ago. Nearly 55% of Canadians stated they have privacy concerns related to social networking sites; however, those who actually used these sites seem less worried – about 45%. Furthermore, only 7% of Canadians read privacy policies. (Office of the Privacy Commissioner 2011).

Surveillance

The ubiquitous presence of surveillance in modern society and the accelerating rate at which technology is developing, has sparked numerous debates amongst many academics. Various scholars (Lyon 1993, 1994; Norris and Armstrong 1999; Haggerty and Ericson 2000) have engaged in critical discussions about Bentham and Foucault's *panopticon*, utilizing it as a metaphor in an attempt to explain modern surveillance. Foucault utilizes Jeremy Bentham's concept of 'Panopticon' to explain how a new kind of society emerged with the rise of the characteristic feature of the modern prison; which is organized in a way that only a few are required to supervise a large number of individuals. Foucault believed that panopticism represents a transformation from a situation where the many see the few, to a situation where the few see the many. He argued that panopticism was transported "from the penal institution to the social body"; our modern society is thus comprised of surveillance activities, where the few see the many, facilitating the furtherance of state and corporate power (Mathiesen 1997, 216-218). Mathiesen, however, critiques Foucault's panopticon, and argues that it is in fact

the *synopticon* which is becoming increasingly manifested in technology. He argues that the nature of our culture is one in which a large number of people can also view the powerful few (i.e., the many see the few). Mathiesen asserts that we live in a viewer society, where both the many see the few while the few can also see the many. (1997, 218-219). In demonstrating the synoptical character of modern society, Rigakos refers to the nightclub as the phenomenon of "getting noticed" which is part of our culture (2008, 218). The nightclub scene is an atmosphere where all desire to see and to be seen, in "the machinery of surveillance" (Rigakos 2008, 186, 188, 218). Inside the nightclub, patrons are scrutinized by bouncers, cameras, and other patrons. A disciplining of bodies takes place, as the few (i.e., bouncers, cameras etc.) watch the many and the many watch the few. (Rigakos 2008, 188, 194).

In addition to the discourses concerning the panopticon and synopticon, other academics propose variations of the panopticon. For instance, Gordon introduces the term *electronic panopticon* in her discussion of the US National Criminal Records System, defining its function of controlling crime as a "panoptic schema", whereby one's criminal record, often incomplete and inaccurate, acts as a surrogate for the inmate and substitutes law enforcement for a warden. Gordon labels this schema, the electronic panopticon, which addresses the current technological developments in surveillance technology that Foucault omits from his literature. (1987, 487). There seems, therefore, to be a consensus amongst scholars (Gordon 1987; Mathiesen 1997) regarding Foucault's argument of the panopticon, in relation to modern surveillance.

Sanchez presents the concepts *cyber-panopticon* and *cyber-synopticon*, to demonstrate the nature of the social networking system Facebook. He argues that the

phenomenon of social networking resulted in problems surrounding privacy control. Consequently, there was an overwhelming response to the perceived intrusion on users' privacy. Users deployed the means by which they were themselves being surveilled (i.e., the cyber-panoptic infrastructure of the Facebook network), to organize an international movement to support their right to privacy. (2009, 275-276).

Haggerty and Ericson, however, criticize surveillance scholars for extending Bentham and Foucault's surveillance metaphor "beyond recognition" in order to account for new technological developments in surveillance (Haight 2007). In response to the quickly developing networks of electronic monitoring and the inadequacies of the panopticon as a model for surveillance discussion, Haggerty and Ericson introduce the concept of "surveillant assemblage", which consists of various technological methods of surveillance that are interconnected in a collection of linkage points (2000, 614-615). Unlike the panoptic and synoptic regimes, the power relationship between the surveillor and the surveilled is levelled in the surveillant assemblage. The assemblage accounts for the observation of both the powerful and the powerless, where the surveillance of each exists in different systems (Haight 2007). Using Deleuze and Guattari, they suggest the growth of surveillance systems is *rhizomic*; like a creeping plant, rather than a central tree trunk with spreading branches (1987, 21). Thus, surveillance is viewed as less centralized yet networked set of processes – a "surveillant assemblage" – rather than as a centrally controlled and coordinated system (Haggerty & Ericson 2000, 614-615). Furthermore, many scholars agree that the surveilled body can be reduced to information, codes; a body double in the midst of the technological assemblage. (Stalder 2002, 121-122; Haggerty & Ericson 2000, 611).

Privacy

Presently, the word privacy is a contested definition amongst various scholars. For instance, Goold (2002, 22) argues that privacy is the liberty to choose how to respond to the demands and curiosity of others, and maintaining some degree of control over the manner in which one presents himself/herself to the world. Goold maintains that privacy rights deserve protection because they are essential for the creation of personal autonomy, and enable individuals to maintain different and valuable social relationships. If one must constantly respond to the expectations of those surrounding oneself, Goold argues, then one's choices are unlikely to ever be free and unlikely to develop the capacity for self-determination or a degree of self-fulfillment (Goold 2002, 22). Stalder, however, argues that privacy is a notoriously vague concept, and disagrees with the idea that it is understood as 'informal self-determination'. He contends that such concept is wrought with ambiguity as it is difficult to avoid entering into relationships that produce electronic, personal data in the public realm and to achieve complete absence from databanks may not be advantageous in any case. Stalder (2002, 121-122) also maintains that privacy is by definition personal, as every individual will have a different notion about what constitutes privacy (e.g., information one disseminates about him-/herself may be personal for one, than for another). Therefore, he claims that it is difficult to collectively agree on the legitimate boundaries of what he calls the assumption of a "privacy bubble". Stalder also raises an important paradox: most people are concerned about privacy, however, most do little to protect it. Such a dilemma indicates that the bubble theory of privacy – based on concepts of individualism and separation – has become unworkable in an environment constituted by a myriad of electronic connections.

He concludes that the bubble theory of privacy is a 19th century conceptual framework applied to a 21st century problem. He proposes instead a re-conceptualization of connections, rather than resistance to them. Rather than viewing surveillance as acts of individual transgression (X has invaded Y's privacy), Stalder suggests viewing them as part of a new landscape of social power, i.e., demanding accountability of those whose power is enhanced by the new connections. In particular, by making the government accountable to those who are governed. He affirms that the current notion of privacy, framed as a personal issue, will not solve the problem. However, notions of institutionalized accountability will address the problem of privacy, as it acknowledges surveillance as a structural problem of political power. (Stalder 2002, 122-123).

This Study in Context

The current state of knowledge about both the development of surveillance technologies and their effect on social relations is large and growing. Entire branches of scholarship, and specialized journals have developed that bring critical scrutiny to the seemingly disappearing idea of privacy. Whatever change might be imagined in terms of the redeployment, reorganization or reform of surveillance and the safeguarding of privacy, however conceived, will ultimately be dependent on citizens' awareness of privacy as a concern. This exploratory study aims to understand whether such awareness and sensitivity to privacy is achievable.

Thus, the impetus of this study is to examine how perception towards privacy, in an era where technology is quickly advancing, might be affected by news of privacy breaches. Is Stalder correct in his assumption that Canadians are ambivalent about surveillance and privacy? Does this ambivalence change with education through news

information? If social attitudes are amenable to change then it is surely the power of media that will most likely affect it. That is, how creating awareness (i.e., of surveillance technologies) through digital media will affect or influence people's way of thinking and future behaviour (i.e., concerning privacy). My hope is that this small study can contribute some empirical context to the ongoing debates, both theoretical and political about privacy and surveillance.

More specifically, however, this study is aimed at exploring perceptions of the impact of surveillance technology on individuals' attitudes towards privacy. Awareness of privacy will be examined in light of various surveillance technologies such as Radio Frequency Identification (RFID), Closed-Circuit Television Cameras (CCTVs), biometrics such as facial recognition software etc. In other words, what and how do individuals living in Canada think and act in defense of their privacy? Surveillance technology is a central aspect of most North Americans' daily lives but we are not entirely clear about the public's attitude towards privacy. What value do we place on privacy? Are we aware of the techniques employed to collect vast amounts of personal information? Does creating awareness of how technological surveillance (e.g., CCTV cameras interfaced with facial recognition software) impacts one's privacy, including the risks involved in disseminating personal information such as fraud and identity theft, change our views towards privacy, and in turn, our behaviour? That is, will individuals become more wary when providing personal information in the future? Ultimately, will people resist providing personal information when requested? Will they take active steps to safeguard their privacy? And, in the end, will they demand that governments, corporations and institutions do the same?

Chapter Two: Theories of Surveillance and Privacy

Surveillance is said to be a condition of modernity, integral to the development of disciplinary power and governance (Haggerty & Ericson 2006, 4). While there are numerous debates about surveillance and privacy, surveillance scholars tend to agree: the concept of *privacy* seems inadequate (Bennett 2011, 485).

Theorizing Privacy

'Privacy' and all it entails is now considered too narrow, too based on liberal assumptions about subjectivity, too implicated in rights-based theory and discourse, insufficiently sensitive to the social sorting and discriminatory aspects of surveillance, and overly embroiled in spatial metaphors about 'invasion' and 'intrusion'. (Bennett 2011, 485). Privacy scholars and advocates have thus expanded the concept of privacy to one which extends beyond social problems; far wider than individual privacy invasion, invoking broader questions of social control aimed at warning us of the dangers of creeping 'surveillance society' (Bennett 2011, 485). Privacy, according to this approach, is seen as protection of the self from organizations and other individuals. Privacy, here, tends to reinforce individuation, rather than community, sociability, etc. (Bennett 2011, 486). For instance, Gavison's (1980, 428) analysis, which posits a possible state of perfect privacy where one is completely inaccessible to others reinforces the notion that privacy is about seclusion and separation. By extension, privacy can therefore only be restored once the entire panoply of public and private organizations stop monitoring and return the information they possess to the rightful owner – the individual (Bennett 2011, 486). Westin (1967, 7) has defined privacy as the claim of individuals, groups or

institutions to determine for themselves when, how, and to what extent their information is communicated to others. Similarly, Fried (1970, 140) also explains privacy as the control one has over information about themselves. Alternatively, the various critiques about privacy and what the term entails have been examined by other surveillance scholars, which have approached the notion of privacy from a different perspective. Lyon (1994, 18), for example, maintains that the issue is not about privacy; rather it is a question of where the human self is located if fragments of personal data constantly circulate within computer systems, beyond any agent's personal control. Regan (1995, 213) argues that privacy should be perceived as a common value, that is, all individuals value some degree of privacy. Bennett (2011, 487) suggests that when privacy is framed in individualistic terms, it is always on the defensive against arguments for the social benefits of surveillance. Therefore, privacy must be framed in social terms, because society is in a better position if individuals have greater levels of privacy. Along the same thought as Bennett, Penney argues that privacy, in the form of anonymity, may encourage people to participate in beneficial activities that they would otherwise not engage in (Penney 2007, 493). Steeves reconceptualises privacy as a dynamic process by which one negotiates personal boundaries in inter-subjective relations. Privacy, therefore, is construed as a social construction that one creates, as he/she negotiates his/her personal relations with others (Steeves 2008, 193). We can categorize privacy further, as Clarke (2006) does, distinguishing between privacy of the person, privacy of personal behaviour, privacy of communications and privacy of data. More and more, privacy is becoming nothing more than a weak rhetorical counter-weight to expanding surveillance.

Theorizing Surveillance

For Bennett, modern privacy issues only partially address the initial process of information collection, capture or relinquishment – assuming a relationship between the organization and the individual. Regulatory problems, therefore, relate to how that relationship is managed in informational terms: how the information is kept secure; how access controls within the organization are managed; how disclosures are controlled, etc. Hence, framing the problem in terms of the conditions under which others may enter one's personal space is not beneficial (Bennett 2011, 489). The public's interest is in controlling excessive surveillance, rather than private interests to protect privacy (Bennett 2011, 490). Bennett claims that privacy is not the antidote to surveillance. It is inefficient to improve privacy laws or attempt to hold government and businesses accountable. It is therefore left to privacy advocates to conduct the empirical work of comparing practice to norms, and holding the processing of personal data to account (Bennett 2011, 494). Perhaps Bennett's lack of faith in privacy is due to what Solove identifies as the concept's disarray. As with the concept of surveillance, it is unclear to Solove (2008, 1) what it means and what it does not mean. Both concepts have been victim to what Sartori (1970) labels 'conceptual-stretching' making it increasingly less possible to identify the range of empirical referents that should fall within their scope (Sartori 1970). Privacy nonetheless frames the way in which most people view contemporary surveillance issues (Bennett 2011, 495).

Yet, another argument surrounding the notion of privacy, is that discrimination is the problem, rather than privacy itself. Individuals are placed at risk because of their membership in certain groups, rather than on the basis of their individual identities and

personal information (Bennett 2011, 490). For Gandy (2009), the problem is not invasion of privacy through the collection of personal information; instead it is the classification and assessment of the information, according to prior assumptions and standard operating procedures. As a result, a power imbalance is created: discrimination is based on classes of people, rather than on individual 'data subjects' (Gandy 2009). Lyon (2003) takes this argument further, identifying the problem of surveillance as social sorting, whereby modern surveillance sorts people into categories, assigning worth or risk, in a manner that impacts or affects their life-chances. Accordingly, surveillance is not merely a matter of personal privacy, but one of social justice (Lyon 2003, 1). Data are extracted from people on a daily basis, as they engage in various informational transactions. Data doubles or digital persona (Clarke 1994) are created from coded categories and serve to open and close doors of opportunity and access (Lyon 2003, 27).

Computerized databases permit marketers to collect, store, update, match, merge and trade information about individual consumers. Accordingly, retailers can make use of extensive amounts of consumer information through technologies that permit data mining and the combining of characteristics into consumer profiles. Merchants now compete by finding out as much information as possible about their customers, and potential customers; and personalizing their marketing approaches based on such knowledge. Companies also utilize this information to categorize and discriminate among consumers; providing better service to more profitable customers. Individuals' personal data has become a valuable commodity that is bought and sold like any other commodity in the marketplace. For example, InfoCanada and Equifax specialize in the collection, enhancement and sale of personal information to marketers, governments, employers and

insurance companies. Individuals are stripped of privacy and control over their personal information. In addition, important decisions are made on the basis of such information; by employers, insurance companies, and governments (Lawson 2005, 2-3, 7). Consider for instance one's personal information contained in a database, which might be inaccurate (i.e., errors in a consumer's profile). If decisions are made based on false or inaccurate information, an individual may be subject to differential treatment. Additionally, the more one is surveilled or exploited by various forms of technology (e.g., RFID, CCTV etc.), the more he/she possesses less control over his/her personal information, and becomes not only vulnerable to crimes such as identity theft, but subject to further control by marketing firms. An individual may never know, for instance, that their insurance application was rejected on the basis of inaccurate information about them in a profile relied upon by the insurer (Lawson 2005, 9). A power imbalance is thus created by this information asymmetry between consumers and the companies profiling them (Lawson 2005, 9).

Some scholars argue that contrary to the idea surveillance technologies (i.e., in the marketing industry) and profiling are means of disciplining and controlling society (i.e., by informing production, marketing and promotion strategies such as direct mailing and advertising); surveillance actually affirms that consumer databases are machines of commodity production, that bring about economic value (Zwick 2009, 240-241). Less cheerily, Neocleous contends that security firms do not engage in the security industry for reasons of 'social control' or 'surveillance'; rather because they have an interest in making a profit (2007, 350). Rigakos (2002) has similarly argued that surveillance is an industry that cannot be separated from a critique of capitalism. Consumer surveillance

captures consumer activities ubiquitously and in minute detail; and databases become repositories of complex consumer lives by turning behaviour into abstract aggregates of individualizing data points. The observation of populations results in the expansion and refinement of strategies of control (Zwick 2009, 221-222). Therefore, the ultimate objective of the deployment of modern surveillance technologies in marketing is the disciplining and controlling of behavioural variations (e.g., detection of 'consumer deviance', followed by marketing intervention) (Deleuze 1992, 3). Such domination and control over consumers does, however, also contribute to the security industry's interest in making a profit.

There are two implications arising from surveillance and social sorting. The first is that the panoptic sort operates in secret. However, there are several mechanisms within the privacy regime designed to achieve transparency. Organizations are expected to notify individuals of the purposes of collection, and must also grant individuals access to their personal information, as well as the ability to correct the information if necessary. Moreover, when companies are monitored, the 'panoptic sort' can be revealed. The second implication of social sorting is the argument that privacy addresses problems of discrete individuals, rather than categories of people. In this case, the privacy regime tends to overlook questions of who gets privacy and who gets surveillance. Another concern stemming from surveillance is the impact it has on vulnerable groups. For instance, one common complaint about the construction of databases without appropriate access controls, is the potential for stalking, especially of young women. Several cases have been documented with respect to airport surveillance practices, health databases, social-networking sites and many others, which suggest that the realm of privacy law is

not concerned with protecting an undifferentiated population of 'data subjects' (Bennett 2011, 491). The proliferation of CCTVs has also led to 'function creep', which is the process whereby a technology is used in an alternative or expanded way beyond its originally intended purpose (Haggerty & Ericson 2006, 19). The aforementioned is one such example, however, surveillance cameras may also be used to blackmail people or perhaps even take advantage of individuals' circumstances. Monahan describes surveillance systems as something which afford control of people through the identification, tracking, monitoring or analysis of individuals, data or systems (Monahan 2010, 8). In addition to CCTV, the use of facial recognition systems also present the possibility of data errors. Individuals may not have access to information which is collected about them, nor the knowledge required to make inquiries about their personal information; and thus no ability to correct erroneous data. There is also no assurance that surveillance information stored for legitimate and justifiable purposes might not be used inappropriately by authorized information gatherers (Gray 2003, 322). For instance, security camera operators at an Australian casino edited visual events captured over the course of four years, onto a videotape which was presented at social gatherings. The videotape included embarrassing and incriminating events (Koskela 2002, 265). Facial recognition technology can target enemies or political opponents (Gray 2003, 322). One must consider the impact that this may have on society. Such actions may create a blackmail society, and incite hate and anger amongst individuals; which could lead to escalating violence.

Additionally, power relations between the watcher and the watched are present, even when personal information is not captured (Bennett 2011, 492). For example, CCTV

cameras need not actually be monitored, or even operational to change behaviour. The potential for surveillance is often sufficient to alter behaviour. Each technological device (e.g., computing devices, remote sensors or drones) structures power relations and imbalances between individuals and between individuals and organizations (Bennett 2011, 492). The privacy regime may produce efficient use and management of personal data however, it cannot control the appetite of modern organizations for more and increasingly refined personal information (Rule et al. 1980). Although the regulation of surveillance technologies cannot guarantee that they will not be misused; it would render it more difficult to establish extensive surveillance networks that facilitate widespread abuse (Penney 2007, 522).

It is becoming ever easier to record anything and everything that one sees, which opens fascinating yet alarming possibilities. In addition to CCTV, recently a new technology has emerged – a device called Google Glass – a wide-angled camera that is worn around the neck and snaps several pictures of one's field of view every minute; recording its location and orientation every time (Economist 2013, 27). A concern arising from this technology, is what if other people are recorded as part of the process? In addition, Glass includes guiding features such as voice commands and head movements that can be used to access a range of data services. Furthermore, Google plans to perch all the functions of a smartphone on the bridge of the user's nose (Economist 2013, 28). Such technology's possibilities would interpose itself between the user and his/her world, including other people. A fear which stems from Glass is that people may surreptitiously use this technology as a teleprompter, perhaps to seem more knowledgeable, which could put at risk the very frankness and honesty of human communications. Another concern, is

the idea that people will inevitably yet unknowingly live on the camera of others. For instance, "creep shots" – furtive pictures of breasts and bottoms taken in public places are a sleazy fact of modern life. Cameras connect more commonly and at times autonomously to the internet, which pose other risks, whereby hackers can remotely control, and use the pictures as blackmail, or for voyeurism purposes. Face-recognition technology, which allows software to match portraits to people, is already used in an obtrusive manner to determine or identify people. (Economist 2013, 28). Imagine for instance that an individual wishes to attend an event or function discreetly, and face-recognition software is used to determine peoples' attendance; would that not be considered an invasion of or intrusion on privacy? What if in turn, the person utilizes that information as blackmail, or to humiliate or embarrass that individual? The potential for abuse is troublesome. If an individual takes a creep shot or looks at someone else's creep shot found online, he/she can determine who he/she is ogling; the practice becomes yet more disturbing (Economist 2013, 29). What if in the world we live in by simply living our lives, we are creating a vast searchable record of all we have seen – a world not, of Big Brother, rather of a billion Little Brothers? (Economist 2013, 29). Does it matter if one's life-log records a stranger on whom his/her eye happens to fall on? Although technology allows for all these possibilities, it does not follow that law and regulation cannot place a check on them. However, checks are unlikely to occur unless demanded. If people have accepted, as Mark Zuckerberg – founder of Facebook – has claimed, that privacy is no longer a "social norm", few people will make such demands (Economist 2013, 29).

Privacy in a Surveillance Society

Contrary to Bennett's arguments in defence of privacy, Gilliom (2011, 500) suggests that the notion of privacy should be abandoned, i.e., that privacy should not be the central theme or terrain for every discussion of surveillance. Gilliom questions whether 'most ordinary people' actually 'see' surveillance; stating that frequently, people seem to be unconscious of the fact that they live in a surveillance-intensive condition, which he terms 'modern life'. Gilliom provides an example of this by explaining that when he informs his students that their cellular phone is a *de facto* location and interaction monitor, or that every credit card transaction records a merchant code, revealing the nature of their business, the students are authentically surprised. Thus, in brief, they do not 'see' the contemporary surveillance issue, or place it in the terms of the privacy framework. Gilliom proceeds to inquire: how must we go about in helping people 'see' the contemporary surveillance issues? To this question, he proposes that it would be more productive for people to consider a new framework; one of social control (Gilliom 2011, 502-503). Haggerty and Ericson maintain that society is organized in terms of risk, surveillance and security, and that surveillance provides knowledge for the selection of thresholds that define acceptable risks and justify inclusion and exclusion. The authors assert that we live in a risk society, governed by institutions that organize themselves through the production and distribution of knowledge of risk. Risk society is fuelled by surveillance; by the routine production of knowledge of populations useful for their administration. Surveillance provides the power to make biographical profiles of human populations to determine what is probable and possible for them; and it fabricates people around institutionally established norms – risk is always somewhere on the continuum of

imprecise normality. The norms emerge from politics of risk in which rules for classifying populations are negotiated. Furthermore, the greater the privacy, the greater the need for surveillance mechanisms to produce the knowledge necessary to trust people; for instance, in institutional transactions. Thus, risk technologies create knowledge-structured inequality (Haggerty & Ericson 2001, 448-451). Surveillance is defined as any focused attention to personal details for the purposes of influence, management, or control (Lyon 2009, 1). Ordinary people's personal data are of interest to others. Agencies process personal data in order to calculate risks or to predict opportunities; classifying and profiling their records on a routine basis. Lyon argues that the use of searchable databases are used for categorizing and profiling, which leads to questions of power involved. Life chances and choices may be affected negatively by the judgments made on the basis of concatenated data. Therefore, raising further questions about social justice, access, risk distribution and freedom. Lyon emphasizes the increased need for ethics and politics of information in an era of intensifying surveillance (Lyon 2009, 1).

Closed Circuit Television Cameras (CCTV [surveillance cameras]), are very prominent in the United Kingdom (UK). The camera has become a permanent fixture within UK society and large swaths of the population are captured on film daily, as they go about their business routines (Sheldon 2011, 193). In Britain alone, there are 4.2 million CCTV cameras; one for every 14 persons in the country; comprising 20 per cent of cameras globally. It has been calculated that each individual is captured on camera an average of 300 times daily (London Evening Standard 2009). In the information age, it is becoming increasingly difficult to lead a life without the constant gaze of surveillance.

Many questions have been raised about the presence of these cameras: Are they simply accepted as the norm by the general public? Do they significantly contribute to public safety? Are they becoming a blot on the landscape, unnecessarily interfering with private lives? What are the social implications? (Sheldon 2011, 193). Findings of numerous studies from both the United States and United Kingdom reveal that CCTV cameras have had little impact on violent crime, and a significant reduction on vehicle crime, particularly when used in car parks (Sheldon 2011, 199). Evaluation to date regarding CCTV remains limited, resulting in calls for an independent review of research evidence on the effectiveness of CCTV for preventing, detecting and investigating crime (House of Lords 2009, 105).

If CCTV systems are increasingly deployed, a psychological sense of being constantly watched will increase amongst individuals; which may have negative unanticipated social consequences (Surette 2005, 164-165). Resorting to a technology solution, therefore, may not only be ineffective, but may for instance, create a sense of alienation amongst people. Individuals may slowly begin to withdraw from the public sphere whenever possible and remain within the comfort and privacy of their own homes. They may become less social with one another (i.e., reduced human interaction), at least in public areas. There may be a spiral of social fragmentation and atomization, leading to more isolation and in turn, more crime. Furthermore, people may also refrain from behaving in a particular way (i.e., in a manner that is not necessarily illegal or abnormal), within a public setting; lest they be recorded by a CCTV surveillance camera and identified as a questionable individual. As Ditton (2000, 707) eloquently states, "... such devices as electronic surveillance represents a significant retreat from [...] collective and

individual responsibility, to self-interest and a culture of fear". The danger is that the expansion of CCTV surveillance may lead to a reduction in the social richness of public space, thereby reducing its potential to be genuinely civilizing and civic (Ditton 2000, 707).

Should individuals have a legitimate expectation of privacy in public spaces? Do privacy rights extend to streets or public areas? Although many people accept that we surrender a certain amount of personal privacy when we enter the public realm, few would concede that we have no expectation of privacy when one walks on the street. However, is it plausible to argue that privacy rights are necessary and should be warranted? According to philosopher David Feldman (1994, 41), privacy rights are important because they provide individuals with the ability to determine and control the boundaries between different interlocking social spheres. For most individuals, one's daily life is lived in a number of social contexts; many of which may overlap. At home one may be a husband, while at work, a teacher, and at a local sports club, a member of a team. In each case, one assumes different responsibilities, responds to different expectations, and maintains different levels of intimacy with those surrounding him/her. Privacy conventions enables one to exert varying degrees of control over the borders between these different spheres, and limits the extent to which he/she is subject to the demands of others within them. While one does not abandon his identity as a husband when he leaves his home every morning, he is not obliged to reveal details about his marriage to his students, or strangers he meets on the street. Privacy is thus, a matter of having the liberty to choose how to respond to the demands and curiosity of others, and maintaining some degree of control over the manner in which one presents

himself/herself to the world. Privacy rights therefore, deserve protection because they are essential for the maintenance of personal autonomy, and enable individuals to maintain different and valuable social relationships. If one must constantly respond to the expectations of those surrounding him/her, his/her choices are unlikely to ever be free, i.e., one is unlikely to develop the capacity for self-determination or a degree of self-fulfillment. The question of whether privacy rights extend to public spaces, depends on whether one can legitimately claim to exercise any control over who shares such space with him/her or how they behave in that space. In other words, does the fact that we appear to have little or no control over the rest of the world in public, mean that we surrender any expectation of privacy when we step into the public realm? Although it is true that we possess far less control over who we encounter in public than when in the home or the workplace, it does not follow that we should be unable to limit the extent to which he/she feels obligated to respond to others' expectations (i.e., controlling space, action, and information) (Goold 2002, 22). Privacy rights should be extended to public spaces, as they serve to protect an individual's legitimate expectations of autonomy.

Closed Circuit Television (CCTV) may be considered a means of creating street-level security in lieu of police patrol. Closed Circuit Television systems are increasingly being built into the urban fabric in the United Kingdom. It seems that protecting spaces of consumption (e.g., the shopping mall) justifies the ongoing use of such surveillance nowadays. However, to examine CCTV is merely to look on the surface of the surveillance-and-commodification theme. Beneath the surface a large industry of personal information processing has arisen that facilitates the capitalist economy more significantly than any other item. These phenomena include loyalty clubs in

supermarkets, frequent flyer point systems, warranty forms that inquire about interests and spending habits, telephone bills, and internet cookies. The common thread amongst these is that they are means of gleaning, amassing, coding, and classifying personal information. A hidden world of personal data processing exists, which places behaviours, preferences, and patterns into categories in order to target marketing efforts more precisely and efficiently. Therefore, the more one consumes, the more is known about his/her consumption, and the more this is used as a guide both to what one will likely consume and to where incentives can be introduced to further encourage that consumption. These practices are known as "database marketing"; whereby personal data are sought wherever they may be found, and entered into searchable databases to be processed into usable information; to produce algorithms that will facilitate the process of matching products to potential customers who have revealed their preferences and past choices. Lyon (2003, 81-85) argues that this is the process whereby consumers are produced for products. Consumers are not programmed to consume in particular ways; rather a range of choices is prescribed. One may argue, however, that over time, in addition to the continuous collection of extensive amounts of individuals' personal information, this may lead people to become programmed to consume items in a particular manner. Technology could be used to amass and arrange one's personal information into databases, to be analyzed and utilized to better understand individuals' behaviours; to devise better marketing strategies to persuade the consumer to purchase commodities. Such strategies may even lead to the creation of additional surveillance technologies that can more accurately capture and analyze consumers' behaviours in the

market; in order to understand them and further control them (i.e., their behaviour – consumption etc.).

In the article titled, *The Way the Brain Buys*, a number of strategies, involving technological advances, which are used by marketers, are revealed; whereby consumers are persuaded to buy items. For instance, to boost "dwell time", i.e., the length of time people spend in a store, mobile phones are tracked by plotting the positions of handsets as they transmit automatically to cellular networks. Research reveals that when dwell time rose by 1%, sales increased by 1.3%. Technology is facilitating the process of monitoring shopper behaviour. Security cameras in stores may be doing much more than simply watching for theft. A company named VideoMining, utilizes image-recognition software to scan the pictures from security cameras, of shoppers while they are making their selections; extracting information such as how many individuals selected one particular brand; compared several items; while simultaneously sorting shoppers by age, gender, and ethnicity. Furthermore, the use of Radio Frequency Identification (RFID) tags, which contain far more information than bar codes and can be scanned remotely, will enable the automatic detection of items placed by shoppers in their trolleys, and charge them to their credit cards. In addition, a store or loyalty card can be fitted with an RFID tag, to identify customers upon arrival. A device placed on the trolley can monitor items that are placed in it; check with past spending patterns, and notify customers who have passed by items which they usually purchase. Radio Frequency Identification tags can also be read at a distance, by anyone with the necessary equipment; which could be used to discover what is contained in one's cupboards at home. Technology will also begin to identify consumers' emotions; as software has the potential to analyze facial expressions. A chief

executive of YCD Multimedia is utilizing digital video screens, displaying ads that relate to what one is buying, and which can also be linked with facial recognition software; to refine the displays according to the customer's age or gender. This system is presently being utilized in Aroma Espresso Bars in America, to present an advertisement for a chocolate croissant, to one purchasing only a cappuccino. Some experts contend that shopping science has limits (Economist 2008, 107); and that it would not be possible to make someone purchase a product they do not need; however, it may persuade them to purchase one commodity over another, without being aware of it. If customers become aware of the psychological methods that are being used to influence their choices, the counteraction may be so enormous, that it can deter him/her from purchasing anything at all (Economist 2008, 105-107). Perhaps shopping science currently has limits. However, in the near future, as a result of the rapid advancements in surveillance technology, in combination with the various methods presently existing and also rapidly developing; which capture, analyze, and produce information, such science may evolve to a point where individuals may purchase products they do not need – where individuals' behaviours will be controlled by the market industry.

The marketer's objective is to "know" the customer. The "knowledge" acquired is merely that of inferred preferences from patterns of consumer behaviour. Marketers use mechanisms to extract and store personal data, for the purpose of creating searchable databases, capable of creating customers. Through means of subjecting the data to sophisticated techniques, profiles of consumers are produced, for use by marketers. Data mining and other kinds of analysis have been added to older methods of data-matching, which enable marketers to make increasingly fine-grained files on consumers. These

profiles can be sorted and ranked in terms of their relative profitability for the corporation; resulting in the differential treatment of consumers. Such practices are becoming more widespread and systematic, leading to the reinforcement of already existing forms of social division and inequality (Lyon 2003, 87). Surveillance techniques are utilized to extract information (i.e., collection of personal data) from, and exploit consumers; resulting in the commodification of personal data, through which corporations can control their consumers.

Corporations exploit consumers by extracting information from them, using surveillance technologies; to better understand the individual, i.e., his/her behaviour (consumption patterns etc.); to further devise strategies to control them; i.e., create new surveillance technologies to extract more information, with the purpose of guiding their behaviour (in daily activities; including the consumption of commodities); while also producing commodities which can further govern their behaviour. The conflation of the commodity with surveillance and risk management, Rigakos (2002) has termed the development of "risk markets" where the expansion of the policing apparatus is part of a wider growth of the security-industrial complex. The intensification of surveillance and the data produced as a result is thus "productive" for capital.

Advertisements are a constant reminder of society's obsession with risk management, safety and security. Television commercials promoting in-vehicle security features are such an example. OnStar is a factory-installed safety and security system that helps keep the driver protected and connected on the road. Equipped with a hands-free, voice-activated phone, it allows one to stay connected more safely while driving. A live specially trained advisor is always available to assist in a major incident such as an air

bag deployment, or in a minor incident (e.g., lockout). The advertisement states, “You'll have peace of mind, knowing you've done all you can to protect your family and prepare for whatever comes down the road” (OnStar 2009). The OnStar security system is an illustration of commodified security, which enhances the attractiveness of the product (i.e., vehicle), while simultaneously instilling emotions of fear, i.e., through the allusion of risks one may encounter whilst driving. It seems that many individuals within society fear the unknown. In attempting to fulfill their desire to protect themselves from any potential risks, they constantly seek security and consequently purchase commodities. Furthermore, where the state fails in providing security for its citizens, the market is provided with an opportunity to expand (Spitzer 1987, 58).

Many people are willing to trade personal information for services. Canadians can expect that privacy will be increasingly commodified and compromised at every opportunity (Ligaya 2013). A 2010 study commissioned by the European Union found that 74% of Europeans stated that disclosing personal information is a part of modern life, and 29% did not have a problem giving up their personal information, in return for free online services, such as e-mail. Approximately 43% of Europeans between the age of 15 and 24 admitted that disclosing personal data is not a problem and 48% also did not mind disclosing their information in return for free online services. However, approximately 70% of Europeans who were surveyed, maintained that they are concerned that their personal information was being held by companies and may be used for purposes other than that for which it was collected. (European Commission 2011).

Nowadays, it seems one cannot expect to have much, if any, data privacy. Experts assert that very little privacy can be realistically expected (Ligaya 2013). Social

networking sites and communication technology make it a simple task for organizations to gather and aggregate information; it is increasingly difficult for one to stay in control of his/her personal data. Organizations have a tremendous financial incentive to collect personal data, because such data is lucrative for them. In addition, spending time in a local shopping mall may also leave individuals unwittingly open to surveillance (Ligaya 2013). A study was conducted of video surveillance cameras in stores and businesses in the Toronto area, and findings showed that most did not follow the rules. Merchants are required to post a sign alerting customers about the camera's use and purpose, and should also display a contact number, in case people would like to inquire about how they can obtain a copy of footage that contains their image. Video surveillance technology is increasingly digitized; computers may be used to analyze images captured by surveillance or CCTV cameras, and identify the people in the footage, using facial recognition software. Businesses may soon be able to alert staff when regular customers visit their store, or market certain products based on their shopping patterns. In these examples power is increasingly centralized to organizations (Brosnahan 2012; Clement & Ferenbok et al. 2012, 358).

Personal data is very valuable not only to organizations, but also to criminals. For instance, a criminal may use one's personal information to impersonate someone, to carry out other crimes such as phishing scams (DesMarais 2012). A case in point is the recent 'Heartbleed Bug', a security bug which compromised large portions of the online world and rendered it more vulnerable. In the internet community, the bug can be exploited, and the attacker can retrieve memory from the remote system. This memory may contain usernames, passwords, or other useful information which enables larger attacks. For

example, an attacker may be able to retrieve information and secrets utilized to encrypt traffic and then intercept and read the communications of all other users of that service. Furthermore, the attacker can connect repeatedly and progressively, and collect more personal information; thus, presenting more internet security risks. (Forbes 2014). Two thirds of the internet servers were affected by the Heartbleed Bug including Australian sites such as the Myer Visa card website and the Coles Mastercard site (Seven News 2014).

In light of our modern surveillance society, therefore, the dissemination of personal information raises many privacy concerns. Stalder (2002, 120) suggests that we live in a type of surveillance society where one's daily interactions (e.g., purchases, withdrawal from ATM machines, etc.) involve the continuous dissemination of personal information. Yet most people are unaware of the consequences of such behaviour, and do not realize the extent to which their privacy is being infringed (Stalder 2002, 120). Throughout the course of one's daily interactions, most of us voluntarily provide personal information such as our telephone number, address, and postal code; almost instantaneously, and without a moment of hesitation, to the requesting party (e.g., store cashier etc.). We leave a trail of data everywhere we go; through bank accounts; itemized bills, listing every credit card purchase; supermarket affinity cards; personal e-mails and SMS messages. Each of us has a shadow self living in the databanks of hundreds of corporations and information brokers; which may contain errors that we can neither see nor correct, and which is constantly examined and managed. When applying for a bank loan, it is one's personal data that determines whether or not the loan should be given. Those who control our data, control our possibilities: they can decide whether we can get

on an airplane, or into a country. Identity theft provides the ultimate proof that control of one's data can lead to control of one's life (Schneier 2008, 61-62). Personal data is collected and processed, and may be utilized to create a profile; which represents the individual's habits and characteristics, and assists as a tool to grant or deny access to particular services (i.e., specialized treatment) (Stalder 2002, 121). Through access to personal information, social control may be exerted upon individuals. The effect stemming from the collection of one's personal information is that, those who 'watch us' know more about us, while we know little about those who 'watch us'. Consequently, an increasing number of institutions have the ability to manipulate individuals, influence their behaviours, and subject them to specialized treatment, in a wide range of situations (Stalder 2002, 121). Society, however, is limited in having access to information about institutions, and therefore, if discrimination were to occur against an individual, he/she would have no knowledge nor know the reason for it; and even if one did, he/she cannot be certain that it is in fact discrimination that is taking place; and thus would be unable to combat it. The possibility of such discrimination is of great concern and problematic, as humans are vulnerable to prejudice and bias, which may result in racial profiling. If institutions can execute decisions in a discriminative manner, and deny individuals a particular service (i.e., while the individual is not aware of the reason why he/she is denied the service), this would constitute a violation of the individual's rights, protected under the Canadian Charter of Rights and Freedoms. Our data is part of us, and we therefore ought to possess basic rights to it and be protected from unwanted and unnecessary examination.

The Rise of Dataveillance

There are two types of surveillance which will be explored in the following paragraphs. The first is visual surveillance and the second, informational surveillance. Visual surveillance entails the surveillance of individuals; utilizing instruments such as closed circuit televisions and facial recognition software, for the purpose of monitoring and collecting information. Informational or textual surveillance will be employed to represent the collection and surveillance of personal data; not derived from nor pertaining to visual surveillance. For instance, the collection and monitoring of personal information contained in various databases (e.g., financial information, name, place and date of birth, race, home address, telephone number, social insurance number, occupation, contacts, criminal record etc.). Informational surveillance can also be utilized interchangeably with the term "dataveillance" or data surveillance, which is defined as "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons" (Clarke 2009). Dataveillance is of two types: "personal dataveillance" consists of the systematic use of personal data systems in the investigation or monitoring of the actions or communications of an identified person; "mass dataveillance" involves the monitoring of groups of people, to identify individuals belonging to a particular class of interest to the surveillance organization (Clarke 2009). Furthermore, dataveillance comprises several techniques such as front-end verification, which is the cross-checking of data in an application form against data from other personal data systems, to facilitate the processing of a transaction; and profiling, a technique whereby a set of characteristics of a particular class of individuals is inferred from past experience, and data-holdings are searched for individuals with a close fit to

that set of characteristics. Unlike electronic surveillance, dataveillance does not monitor the individual, but merely the shadow that the person casts in data. The term "digital persona" reflects the model of an individual's public personality based on data, which is maintained by transactions; and is also used as a proxy for the individual (Clarke 2009). However, like any mere model, a digital persona is a partial and inaccurate reflection of a complex reality.

The fusion of visual surveillance and informational surveillance gives rise to several implications. Facial recognition systems can connect to digital surveillance cameras, which can then be used to monitor spaces for the presence of individuals, whose digital images are stored in databases. Images of those present in a space under observation can be recorded and subsequently paired with identities (Gray 2003, 316). For example, facial recognition software can be used to scan a crowd of individuals present at a political conference, to identify which delegates are present, and which are not. Facial recognition has the ability to reach quickly into the past and retrieve information; which dramatically extends the effective temporal scope of surveillance data analysis (Gray 2003, 317). Once an image is included in a database, stored surveillance data can be searched for occurrences of that image, simply with a few keystrokes. Yet, several problems arise when information is networked. Discrete pieces of information about an individual may be relatively harmless to privacy; however, when information is shared, a comprehensive dossier on the individual can be assembled (Gray 2003, 316). Useful here, is Haggerty and Ericson's (2000, 614-615) concept of the "surveillant assemblage"; defined as the various technological methods of surveillance that are interconnected in a collection of linkage points. Surveillance power expands as various

systems, both public and private, are networked together to share information (Gray 2003, 316). Once an individual has been identified by a facial recognition system, his/her profile can actually be compared with banking data, as well as criminal background information; which makes personal privacy an open book for those seeking the information (Idanan 2009). Concerns have been raised that a single biometric could be used to access vast amounts of personal data held on different systems; including ones managed by authorities. Consequently, if more biometric information is circulating in insecure areas, there is an increased risk that it may be saved on memory sticks and accidentally left in a public area, or sent somewhere on a compact disc and lost (Thomas 2009). When technologies of visual surveillance are integrated with facial recognition software, they eliminate anonymity; and when converged with databases, the traditional notion of a Big Brother State (i.e., surveillance state), seems to be in effect.

Academics have identified a serious consequence arising from the implementation of surveillance technologies. Searchable databases generated by biometrics such as facial recognition software, may be used as tools of oppression; facilitating intensive processes of "social sorting", whereby processes of exclusion and inclusion are deepened and extended (Wilson 2007, 213; Norris et al. 1999). Closed circuit television is a technology of control; and when it is interfaced with other technologies such as the internet, face-recognition software and databases, its power increases substantially (Davies 1999, 1; Gray 2003, 316).

The combination of closed circuit television, facial recognition software, and personal data (i.e., visual and textual surveillance), can perhaps be utilized to produce yet more personal information on individuals, so as to build a comprehensive profile of each

individual. Such unification may also be used to attain particular objectives. Closed circuit televisions, in conjunction with facial recognition technology, may identify faces, understand body language, and respond to facial expressions. Subsequently, interpretations or translations of such large quantities of information could then be exercised by those in control, perhaps in an unethical manner, for their advantage. Facial recognition has the potential to create permanent digital records of daily activities, granting observers the opportunity to interpret actions and motivations across lengthy periods of time; resulting in mistakes becoming permanent (Gray 2003, 323). Individuals frequently infer ideas about others based on limited evidence, i.e., often involving a lack of context and knowledge, as well as confusion regarding information. In other words, the meaning of one action or piece of information can be erroneously utilized as proof that knowledge has been revealed about one's character. Visual information thus could be used in various ways to demonstrate which category an individual belongs to contrary to other forms of surveillance (i.e., textual surveillance), which often identifies what an individual purchases, or his/her involvement in different activities. A picture does not always reveal the context of a given situation particularly whether or not it is an isolated incident (Gray 2003, 324). Consider for instance a hypothetical situation, whereby a woman repeatedly strikes her child. The woman was also in the midst of a stressful period in her life at that moment, and her child was having serious disciplinary problems. Suppose that she had never hit her child, and was overwhelmed with grief immediately after the incident. The camera does not display any of this. In a surveillance society, a single action can categorize an individual (Gray 2003, 324). The mother's actions may be stored permanently, and used against her at a later point in her life; perhaps to further

demonstrate the kind of individual she "is". Authorized individuals could also manipulate technology to their advantage. Consider yet, another hypothetical scenario, whereby an accused individual is on trial for a particular offence. During the course of the investigation, authorities discover what appears to be, relevant visual information (e.g., depiction of unusual behaviour), and infer that it accurately displays the character of the accused. The information could in turn be used for the purpose of securing a conviction, and in other cases, apprehending, or charging an accused; who may not be the actual offender. Other authorities could corrupt technology, i.e., alter visual information to accomplish the same task. Whether or not such evidence would be admissible in court, is beyond the scope of this thesis. Consider the impact such information might have, if merged with personal data (i.e., that which is derived from informational surveillance). The outcome may be quite detrimental. More information may be produced about the character of the accused, much of which may be unfavourable to him/her; subsequently resulting in a wrongful conviction.

There is a danger in viewing visual and informational surveillance as two distinct types of surveillance. Individuals must become aware of both existing types of surveillance, as they function together. As previously examined, there are many risks associated with these methods of surveillance. The technologies used to conduct visual and informational surveillance present unique problems of their own, and are far from being addressed. The combination of both techniques of surveillance thus, not only compounds existing issues, but creates a whole new set of problems that are more complex in nature. The failure in noticing the connection between visual and informational surveillance will lead to greater concerns that will be difficult to address.

As technology continues to develop and increase in complexity, so will the nature of our problems. Privacy may cease to remain a part of our lives, as there will be greater opportunities for any one individual to be surveilled via numerous databases containing visual and textual information; there will be greater possibilities for discrimination and profiling, amongst other concerns. Society seems to be unaware of this connection, and as such, will have greater difficulty defending their privacy in the future. Oblivious to the available technologies that can accelerate the collection of personal information; individuals are heading towards a transparent surveillance society; one which will lead to the demise of their privacy. Consequently, a more serious problem may arise from such linking, and collection and analysis of extensive amounts of personal data. Patterns of behaviours could be observed of the general population under surveillance; which could then be used to make determinations regarding what consists of "normal" and "abnormal" behaviour. Profiles could then be created accordingly, to classify individuals into two kinds: those who are "normal" and those who are "abnormal". Recorded information could also be used to make predictions about particular types of behaviours; by finding common underlying characteristics among the general population, so as to further segregate them, for the purpose of identifying those who pose a "risk" to society.

There are several implications surrounding facial recognition software. Security experts claim that storing such data on both government and privately owned computers poses an increasing threat to individual privacy, and opens up new frontiers in identity theft. The major problem in using biometrics for identification purposes is that even if they are encrypted, they need only be hacked once to be compromised forever (Anderson 2009). Although there have been advancements in technology, which make it more

challenging for a criminal to forge another person's identity, a criminal may go to great lengths to achieve their goal. Perhaps the following example may no longer be possible to use, due to the now complex and advanced state of technology; however, a few years earlier, it may have been a simpler task to steal one type of biometric. Imagine a remote system that utilizes facial recognition as a biometric (Schneier 1999). Suppose that in order to gain authorization, one must mail a picture of himself/herself. If someone takes a picture of you without your knowledge and submits it via mail, one might be able to fool the system. Although it is difficult for someone to make their face look like yours, it is simpler to obtain a picture of your face. The system does not verify when and where the picture was captured; only whether it matches the photograph of your face which is stored in the database. A keyboard fingerprint reader can also present similar problems. If verification occurs across a network, the system may be unsecure (i.e., the connection from the reader to the verifier). A criminal will not attempt to forge one's real thumb, but rather will try to inject one's digital thumbprint into the communications. Thus, biometrics are a useful tool only if the verifier can confirm that the biometric originated from the person at the time of verification; and that it matches the biometric on file. If the system cannot execute such tasks, then it may function in a contrary manner that may not be advantageous to the user (Schneier 1999). Consider this same scenario in a slightly different context; whereby instead of attempting to gain authorization (e.g., to access a particular location or restricted area), one attempts to access a database containing your personal information, while using the same method described above. If the criminal is successful in doing so, he/she may use that information to perform criminal activities,

such as stealing your identity. Security experts must therefore, devise systems for security applications, as some people will aim to circumvent them (Schneier 1999).

A study of the acceptance of biometric security services (Heckle & Patrick et al. 2007) reveals that there are differences of opinion, when the perceived benefits for the users were manipulated. Participants indicated higher acceptance when the biometric was used to secure personal information for personal purchases; in contrast to securing personal information for corporate purchases. There were 22 references to privacy from 13 participants who voiced their privacy concerns explicitly, stating that biometrics are invasive; while others believed that privacy concerns were not important. What is notable for this thesis is that researchers concluded that there was participant hesitation due to insufficient knowledge of the technology or its ramifications.

Privacy, it has been said, is an essential prerequisite to the exercise of individual freedom (Travis 2009). If we are observed in all matters, if we are constantly under the threat of correction, judgement, criticism, and even plagiarism of our own uniqueness we may become constantly fearful that patterns we leave behind will be brought back to implicate us, by whatever authority has become focused upon our once-private and innocuous acts. We lose our individuality because everything we do is observable and recordable. This is the loss of freedom one is faced with when privacy is taken away from him/her. The long-term effects of this on society are toxic – we give up control of ourselves (Schneier 2008, 61-64).

We know that individuals are not adequately informed of the consequences in disseminating personal information – that is, both the short- and long-term consequences. People are not in a position to make informed judgements, and information is often out of

their control (Clement & Ferenbok et al. 2012, 356). Therefore, perhaps by creating awareness of the privacy risks or consequences involved in voluntarily disseminating personal information, and the various existing surveillance technologies; people will be adequately informed and equipped to protect or control their personal information. In modern society, the increasingly complex and quickly advancing technological developments facilitate the collection of personal information, and contribute to social control. Surveillance is ever-present, and the state and corporate sectors are utilizing technological tools at their disposal to exploit individuals; by extracting their personal information, to further control them, and guide their behaviour. Are we sleepwalking into a surveillance society? Have the tools of mass surveillance become so ubiquitous that notions of individual privacy are a thing of the past? (Parliamentary 2009). I would argue that there is an urgent need for society to take the potential pitfalls of surveillance seriously. Perhaps it is only a matter of time before we become consumed in the consumption of commodities and caught in the web of surveillance technology. This ought to give us pause to think before consuming, to reclaim control over our personal information. As Harris asserts, "The greatest danger in modern technology is not that machines will begin to think like people, but that people will begin to think like machines" (Thinkexist Quotations 1999). The premise of this exploratory study, therefore, hinges on the idea that in order for social change to take place, we need an informed citizenry. Even though we are experientially saturated with surveillance, dataveillance and risk management to the likely demise of privacy, we are often unaware of these processes at work. Perhaps this ought not to be a problem but we ought to at least explore whether awareness of these broader issues are important to us. Before any

debates about privacy can take place we ought to first determine whether knowledge of the excesses of this regime of surveillance matters to us.

Chapter Three: Methodology

This is an exploratory study measuring the effect of viewing previously televised news reports and documentary clips on awareness and sensitivity to privacy. The study seeks to understand the immediate short-term effects of such an exposure on people's way of thinking and potential future behaviour in safeguarding their privacy. Respondents were placed into two groups – control and experimental – and then asked to fill out a survey that asked about their experiences, attitudes and precautionary practices with respect to privacy.

Respondents

As the research study involves human participants, permission was first requested from the Research Ethics Board (REB [on December 3, 2012]), and was subsequently received. A hardcopy of the questionnaire (**Appendix B**) was administered to a semi-random and representative sample (i.e., with regards to gender, age, etc.) of 60 Carleton University students. Initially, attempts were made to recruit participants through requests from professors within the Department of Law and Legal Studies. My hope was to recruit during class time so that I might present the nature of the research study for the purpose of obtaining student respondents. However, this method of recruitment was unsuccessful. As a result, participants were recruited through solicitation on the Carleton University campus.

On April 17th, 2013 I set up by the cafeteria in the Unicentre but only two participants were recruited to view the video and answer the questionnaire between the hours of 12:00 pm and 5:00 pm. The take-up improved when I moved outside the Azrieli

Theatre and the Tory building on April 22, 2013. Thirty-nine questionnaires were administered between the hours of 10:30 am and 6:00 pm; 9 of the participants viewed the video beforehand. On April 24, 2013, 7 questionnaires were administered to participants who watched the video (between 10:30 am and 5:30 pm – by the Azrieli Theatre). Finally, on June 4th, 2013, a total of 12 participants were recruited near the cafeteria; they viewed the video and completed the questionnaire between the hours of 10:00 am and 4:30 pm.

The control and experimental groups consisted of 30 respondents each for a total of 60 participants. While students were randomly assigned to the two groups, their selection was not random as it was dependent on face-to-face recruiting on campus. Approximately 30 minutes was required to administer the questionnaires to the control group, and approximately one hour was required, on average to administer the video and questionnaires to the experimental group (i.e., 30 minutes to view the video and 30 minutes to complete the questionnaire). Incentives such as coupons, gift certificates and treats/food (e.g., chips and soft drinks) were used to recruit participants. Prior to completing the questionnaire, or viewing the video and completing the questionnaire, each participant was provided an REB Consent Form (**Appendix C**), which outlined the purpose of the research study, and what is entailed in the study, e.g., the length of time it will take etc. The Consent Form explains the participant's right to withdraw from the study; confidentiality and anonymity; the implications and benefits of the study, as well as how their data will be collected and stored. The Consent Form must be signed by both the participant and researcher, and dated prior to the subject's participation in the research study.

Data collection consisted of two stages. In the first stage, the questionnaire was administered to a random sample of Carleton University students (i.e., 30 students) – the control group – who was not exposed to the condition (i.e., video clip). In the second stage, 30 other students who were randomly selected as participants – the experimental group – were exposed to the condition, wherein they viewed an educational video clip (presented on a laptop, on the Carleton University campus) – the duration of which is 26 minutes. The video content includes news and documentary clips concerning various methods of surveillance technology that are used to collect one's personal information; how such information can be used to classify individuals; and the risks involved in voluntarily disseminating personal information. The video clip includes excerpts from various news-related articles and videos which have been presented in the media and illustrates the importance of privacy, the consequences arising from inadequate protection of personal information, surveillance, technology and its ramifications, as well as the future of privacy. Subsequently, the participants completed the same questionnaire as the control group.

There are limitations in administering questionnaires to Carleton University students. Inferences may be drawn about how teachable the population is or that they may be a specific and non-representative subset of the population. I make no claims about the generalizability of the results. They are, after all, exploratory in nature and aimed at answering a more modest question: can conveying televised news stories about privacy and surveillance raise awareness and affect concern about privacy (in any population)?

Questionnaire

The questionnaires consist of multiple choice questions, yes/no questions, Likert-scale questions, and five open-ended questions to allow for participant insight and further comments or opinions. The questionnaire has a total of 44 questions. At the end of each questionnaire, an additional form was included to collect statistical information about the participant e.g., gender, program of study, etc. (**Appendix B**). The questionnaire was created to test whether the information covered in the video concerning privacy, surveillance technologies, collection and dissemination of personal information, social networking sites, etc. had an impact on the respondents. The questionnaires were randomly assigned to both the control and experimental groups of participants.

The Video

The video entailed information about Closed Circuit Television (CCTV) surveillance; biometric software such as Facial Recognition Software; social networks such as Facebook, and the interfacing or conjunction of at least two of the three. The video also discussed Radio Frequency Identification (RFID) technology, electronic payments and data mining.

The video was created using a program called Nero. Some of the links which were included in the video are available in **Appendix D**; which includes news footage (e.g., abc news, CNBC), i.e., interviews with professionals, reporters and privacy advocates etc. A slide show was also incorporated into the video. The 26 minute video focused on the importance of privacy in modern society, and offered information about various surveillance technologies currently being used in North America including CCTV, RFID, biometrics, and so forth. The video was created and compiled using various sources; it

includes PowerPoint slides, and was edited several times (the information, i.e., slides and edited versions of videos were fused together to create a short educational video). The video is divided in the following ordered segments:

- Slide 1: Introduces modern society, in light of technological advancements. (00.00 – 00.02 minutes).
- Video clip 1: How is Big Brother Watching You? (compilation of three clips) (00.03 – 01.46 minutes). Source: CNBC Prime, October 18, 2006
- Slide 2: Biometric Technology (01.47 – 01.49 minutes).
- Video clip 2: No Place to Hide – Part One (compilation of six clips) (01.50 – 07.59 minutes). Source: abc News, April 28, 2007
- Slide 3: Biometric Technology: Iris Recognition (08.00 – 08.02 minutes).
- Video clip 3: Big Brother's Face and Eye Recognition Software (compilation of nine clips) (08.03 – 11.03 minutes). Source: UK: CyLab Biometric Centre, 2010
- Slide 4: Biometric Technology: Facial Recognition Software (11.04 – 11.06 minutes).
- Video clip 4: ISS Facial Recognition Security Software Highlighted on Fox News (compilation of three clips) (11.07 – 13.32 minutes). Source: FOX News – APB Tech, April 7, 2010
- Slide 5: Another Type of Surveillance Technology: CCTV (13.33 – 13.36 minutes).
- Video clip 5: Big Brother Literally Watching you and Talking! (one clip) (13.37 – 14.28 minutes). Source: British News, Daily Planet, April 1, 2008

- Slide 6: In addition to surveillance technologies… (14.29 – 14.31 minutes).
- Slide 7: Do you have a Facebook account? (3 consecutive slides: 14.32 – 15.14 minutes).
- Slide 8: Recently a new Facebook feature has been added… (15.15 – 15.18 minutes).
- Video clip 6: New Facebook Feature – Cool or Creepy? (compilation of two clips) (15.19 – 19.39 minutes). Source: abc News, June 10, 2011
- Slide 9: RFID Technology (19.40 – 19.42 minutes).
- Video clip 7: How RFID Works (one clip) (19.43 – 21.37 minutes). Source: CBN, Realpsychichere, January 1, 2007
- Slide 10: How is RFID being used? (21.38 – 21.41 minutes).
- Video clip 8: RFID is pretty cool technology, but is it safe and secure? (one clip) (21.42 – 23.34 minutes). Source: Brainphreak, April 21, 2009
- Slide 11: Data Double chart (23.35 – 23.57 minutes). Source: Course notes, 2010
- Slide 12: One of the many consequences… (23.58 – 24.01 minutes).
- Video clip 9: Who Knows Your Secrets? (one clip) (24.02 – 26.00 minutes). Source: CNBC Prime, October 18, 2006
- Slide 13: Are you in control of your personal information? (26.01 – 26.06 minutes).

The video begins by discussing biometrics, and introduces devices such as iris scans and palm scans. These devices capture the landmarks / details of one's face, from which a mathematical equation is then created, to determine one's identification. The

video explains how some technologies accumulate information about an individual, then mine that individual's data (gathered from various sources) and sell the information to others. Based on the personal information gathered, companies can study what people are likely to do; study their attitudes based on their purchases, how they are dressed and where they travel; they can determine the value of the house one resides in, and the kind of car one drives. Many of these companies have both, computer intelligence software and analysts who aggregate and derive conclusions from that data.

The video then presents Axiom – a company which collects and manages information for credit card companies, insurance companies and banks. Axiom ultimately assists other companies in better understanding their customers. The participants were then exposed to supercomputers and data-mining, which teaches computers to do the same type of analysis that a human being would, if humans could analyze a million pieces of data in one second. ChoicePoint is another similar company, which absorbs information from 40,000 new public records on a daily basis. ChoicePoint possesses 20 billion records on all adults in America, and works with intelligence agencies. A ChoicePoint representative made the following statement in the video: "One has the right to privacy, but not anonymity." A privacy advocate disagreed with the representative's statement and explained how such companies collect one's personal information and sells the information to other companies who can then make inferences and decisions about those individuals from whom the information was collected – it is a marketing business.

The next segment of the video explains iris recognition – software which analyzes one's face and records information or details about an individual's face, in order to determine the person's identity. In combination with CCTV (Closed Circuit Television)

cameras, this technology – used in the United Kingdom – can recognize, identify individuals and follow one's every move.

The following portion of the video describes how facial recognition software functions – it can identify individuals in conjunction with CCTV cameras, even if one is moving (i.e., one does not need to be standing still). The counterargument to the fact that such technology is an invasion of privacy is that nowadays everyone is on Facebook, and it is only the features of one's face, i.e., vector data which is recorded.

The next clip in the video demonstrates how talking CCTV cameras are used in Britain, as a deterrent. The subsequent section of the video informs participants about a Facebook feature – facial recognition technology – which is applied, when one uploads pictures to Facebook. The feature entails capturing and recording the biometric fingerprints of one's face, which Facebook then stores and uses, to recognize and identify individuals. A critic commented on this feature; believing that Facebook's interest is to try and encourage its users to disclose more information about themselves than they might otherwise not choose to disclose.

In the following segment of the video, Radio Frequency Identification (RFID) is explained as a tiny silicone computer chip and antenna that a remote reader can scan, and send information to a database. Examples are provided where retail stores such as Wal-Mart (in the United States) requires suppliers to track its products. RFID chips render objects trackable and can easily be concealed in fabric or clothing. Therefore, people and objects can be numbered and tracked; every move one makes can be identified and logged in a computer database, which raises questions about power. Implantable RFID chips (size of a grain of rice) can be imbedded in humans, to monitor population. RFID

waves can travel through walls, wood, purses etc. – all objects on which individuals rely to protect their privacy. Another scenario which was presented in the video, is the possibility that RFID chips could be inserted into cash, which would create an audit trail thus removing the anonymity one has when using cash.

Participants were then educated on the concept of a *data double*, where the body becomes reduced to pure information. The final section of the video reports an incident which happened to a doctor, whereby her personal information was compromised due to a breach of information at ChoicePoint – a company who collects and stores information about individuals' dates of birth, telephone number, bank account information, social security number etc. The doctor who was a victim of this breach was negatively affected, as she could not, for instance, apply for credit etc.

Analysis

The results of the first questionnaire (i.e., administered in the first stage), establishes a baseline comparison to determine whether the video resulted in any impact on the participants. The results from the questionnaires from the control group were aggregated, analyzed, and compared to the results generated from the questionnaires which were administered to the experimental group. This statistical comparison between groups forms the basis of the empirical contribution of this exploratory study – to determine if there was an association between participants' attitudes towards privacy, and their awareness of surveillance technologies employed to gather personal information dependent on whether they watched the video.

The data was recorded and analyzed using the following software: Microsoft Excel spreadsheet and the Statistical Package for the Social Sciences (SPSS). Two

separate Excel spreadsheets were created, to capture the data collected from the completed questionnaires. The first spreadsheet included data gathered from the control group, and the second spreadsheet contained data collected from the experimental group. Once all the data were entered into each corresponding field, they were coded (e.g., 1 = Yes; 2 = No), in order to export it into the SPSS database. The coded data were then inputted into SPSS, to begin statistical analysis.

Chapter Four: Results

Two groups participated in the research study. The first group (the control group) did not watch the video, and only completed the questionnaire. The second group, (the experimental group) viewed a 26 minute video aimed at sensitizing and informing them about privacy concerns and the protection of personal information. The experimental group then completed the same questionnaire as the control group, with some additional questions aimed directly at their impressions of the video.

Awareness

Respondents were asked to check as many terms as they felt appropriately made them think of privacy from a list including:

- Confidentiality of personal information;
- Secrecy/others not knowing your personal information;
- Security/protection/encryption/passwords;
- Home/family/bedroom;
- Being left alone/no solicitation/seclusion;
- Invasion/lack of privacy;
- Confidentiality of your personal information (companies);
- Confidentiality of your personal information (Internet);
- Tracked by government;
- Freedom/Non-interference/Anonymity;
- Other – please specify.

There was no statistically significant difference between the control and experimental groups in associating these listed terms with privacy. It is particularly striking that none of the terms solicited any differences between groups indicating that a general understanding of the connection to privacy and the terms exists regardless of exposure to the video. (see Appendix E, Table *2*).

As noted, the groups were not entirely randomly assigned as respondents were recruited on an ad hoc basis. For this reason it is reassuring to note that there was no statistically significant difference between groups in terms of their tendency toward taking precautions to safeguard their privacy. Question number 2 asked "Do you take any measures or precautions to protect your personal information?" 83.3 per cent of the experimental group and 90.0 per cent of the control group reported that they took precautions to safeguard "any information about an individual's identity, ranging from name, age and address to health history, employment status and income" ($X^2 = 0.577$, p = *ns*, see Appendix E, Table 3a).

There was a strong, statistically significant difference between control and experimental groups in their knowledge of Radio Frequency Identification Technology (RFID) /tagging, ($X^2 = 9.600$, $p < 0.01$). A total of 9 respondents (out of 30 or 30%) who did not view the video had knowledge of RFID technology; whereas, as expected, following exposure to the educational video, most participants (21 out of 30 or 70%) reported an awareness of RFID tagging. Similar results were found with knowledge of Biometrics ($X^2 = 21.696$, $p < 0.01$). Of the individuals who completed the questionnaire, 7 out of 30 (23%) were aware of Biometric technologies; whereas 25 of the respondents

(out of 30 or 83%), who were exposed to the video became aware of Biometrics. [Questions 7 and 8] (see Appendix E, Tables 6 and 7).

A significant difference was observed between the two groups with respect to their knowledge of specific technologies (i.e., RFID, Biometrics, Closed Circuit Television, Global Positioning System), ($X^2 = 5.455$, $p < 0.05$). Of the 30 individuals who completed the questionnaire, 5 answered "none of the above" which means that they had no knowledge of any of the aforementioned technologies. On the contrary, none of the participants who viewed the video scored "none of the above"; thus, implying that after watching the video, all of the participants gained knowledge about one or more of the aforementioned technologies that they likely did not have. [Question 7e] (see Appendix E, Table 6).

There was also a statistically significant difference between groups concerning their knowledge about privacy and surveillance including terms such as "data double" ($X^2 = 15.022$, $p < 0.05$). All the participants in the control group, except for one, were not aware of the term *Data double*. In contrast, 14 of the 30 respondents who watched the video, were aware of the term *Data double*. [Question 8a] (see Appendix E, Table 7). There was also a strong association between watching the video and the feeling of possessing less control over their personal information ($X^2 = 6.667$, $p < 0.05$). However, there was no significant difference between genders, as might be expected, on the same measure (X^2 (1, 55) = 0.667, $p = ns$). [Question 25] (see Appendix E, Table 3b).

There was also a relationship between watching the video and changes in perceptions of privacy ($X^2 = 60.00$, $p < 0.05$). [Question 33] Here, there was some evidence of a difference between genders on perceptions of privacy ($X^2 = 4.929$, $p <$

0.05). Albeit a small sample, out of 20 females surveyed, only one indicated that her perception or view of privacy has not changed after having viewed the video; whereas only three of the eight males surveyed indicated the same. [Question 33]

Table 1. *Changes in Perception of Privacy After Viewing the Video*

	Yes	No	Total
Male	5 63%	3 38%	8 100%
Female	19 95%	1 5%	20 100%
Total	24 85.7% 100%	4 14.3% 100%	28 100% 100%

Following the viewing of the video, the majority of participants in the experimental group – regardless of gender – indicated that their perception of privacy has changed. The evidence seems clear, although perhaps not surprising, that creating sensitivity toward privacy is possible when respondents are exposed to an educational video concerning existing surveillance technologies which leads to changes in perception about privacy. A factor which may have accounted for the higher number of women positively responding to this question, is the segment of the video that recounts how two women were victimized by identity theft, fraud and the inaccuracy of personal information, which led to being denied a job on several occasions.

Social Networks

There was a statistically significant difference between genders on the use of social networking websites such as Facebook, and their privacy settings (X^2 (2, 55) = 7.543, $p < 0.05$). Out of 55 respondents – 20 males and 35 females – 4 males and 1 female used Facebook or other social networking websites, but do not use the privacy

settings. A total of 16 males and 28 females used Facebook or other social networking websites, and employed the privacy settings to set restrictions to their profile. All of the male respondents used Facebook or other social networking sites (see Appendix E, Table 11).

Personal Information

The experimental group was significantly more likely to believe it is not possible to maintain a degree of control over one's personal information (i.e., three quarters of the group, *(*$X^2 = 7.500$, $p < 0.05$). Nearly all of the respondents from the control group (25 out of 30) believed it possible to maintain a degree of control over their personal information. [Question 26a] (see Appendix E, Table 3b). Those who scored "yes" to the previous question (26a), also believed they currently have a degree of control over their personal information (X^2 (2, 60) = 7.724, $p < 0.05$). The control group maintained a stronger belief in this regard. [Question 26b] (see Appendix E, Table 3b).

Participants were asked to rate on a scale, from "Very Poor" to "Very Good", how well they believe they are doing in protecting the privacy of their personal information on a daily basis. There was no statistically significant difference between the two groups (t (58) = 1.401, $p = ns$). [Question 3] (see Appendix E, Table 9). One might have expected there to be a difference between the two groups as the participants who viewed the video may have come to the realization that they are not doing as well as initially thought in protecting the privacy of their personal information. Nonetheless, the group that watched the video believed they had less control over their personal information than the control group, who did not view the video (see 26b above).

Concerns with Technology, Privacy, and Protection of Personal Information

There was no significant difference between control and experimental groups regarding sensitivity toward the potential of being a victim of identity theft ($X^2 = 0.131$, $p = ns$). [Question 10] This held for both men and women (X^2 (1, 55) = 1.713, $p = ns$). [Question 10] (see Appendix E, Table 3a). Question number 23 asked participants to rate the degree to which they agree or disagree with the following statement using a 7 point scale, where 1 means *strongly disagree*, 7 means *strongly agree* and the mid-point 4 means *neither agree nor disagree*. The statement is as follows:

(a) I think the claims about the negative consequences of technology on the protection of personal information are overblown. [Question 23] (see Appendix E, Table 10)

There was no statistical significance between groups. The mean value for both groups scored between 2 and 3 (close to 4 – "Neither Agree nor Disagree").

Subjects were also asked to rate (on a scale from 1 to 7) the following question: "I am concerned about the privacy and protection of my personal information?" [Question 24] (see Appendix E, Table 10). There was no statistical significance here either. The mean value for both groups scored between 5 and 6, where a score of 7 indicates "Strongly Agree".

Accuracy and Access to Personal Information

Participants were asked whether they are concerned about the level of accuracy, or misinformation contained in their personal files, which may be held by various institutions. There was no statistically significant difference between groups. Both the

control and experimental groups scored a mean value of 4 – "Somewhat Concerned" (less than 5) on the scale. [Question 29] (see Appendix E, Table 1). Respondents were also asked about their concerns about who views, or accesses their personal information. Once again, no statistically significant difference was evident, and both groups scored a mean value of 5 (between 4 – "Somewhat Concerned" and 7 – "Extremely Concerned"). (see Appendix E, Table 1) [Question 30].

Impact of Technology on Privacy

An independent-samples *t*-test revealed a statistically significant difference between groups on the extent to which technology may have a negative impact on their privacy (t (58) = -2.854, $p < 0.05$). The results reveal that the experimental group was more concerned with the impact of technology on their privacy. [Question 9] (see Appendix E, Table 1).

Question number 6 asked respondents to check as many of the following terms which they were most concerned about, regarding technologies and privacy issues: [Question 6] (see Appendix E, Table 12).

- Hacking technologies/invasion of privacy/identity theft (unprotected databases, hacking into company/government information, transaction information, information not being protected by companies/government);
- Internet/computer use (general mention includes mentions of electronic and wireless technologies);
- On line social networking sites/music, video, chat (Facebook, You Tube, chat rooms, gaming sites);
- Banking/on line banking;

- Use of cell phone/telecommunications technology/handheld devices, Personal Digital Assistant (PDA's), Blackberries, mobile devices;
- Credit cards/debit card concerns of transaction/use (cards in general);
- Companies/Organizations selling information/sharing information/misuse of information (includes data mining, telemarketing, soliciting, includes do not call lists being misused);
- Surveillance/tracking/recording technologies (card/licence chip technology, satellite, GPS, cameras, phone tapping, RFID's, smart cards);
- Others – please specify;
- I am not concerned with any technologies impacting my privacy.

The only statistically significant difference between the control and experimental groups with regards to the most concerning technologies, in light of privacy issues were the "Use of cell phone/telecommunications technology/handheld devices; Personal Digital Assistant (PDA's), Blackberries, mobile devices" ($X^2 = 5.455$, $p < 0.05$); and "Surveillance/tracking/recording technologies (card/licence chip technology, satellite, GPS, cameras, phone tapping, RFID's, smart cards)" ($X^2 = 5.934$, $p < 0.05$). Thirty per cent of the control group selected the former, whereas double (60%) of the experimental group selected the former; thus displaying the experimental group's great concern, more than that of the control group's. With regards to the latter statement (i.e., surveillance/tracking/recording technologies), half (50%) of the control group selected this option, whereas nearly double (80%) of the participants from the experimental group selected this option as the most concerning technology which may affect their privacy. Therefore, the group who watched the video was statistically significantly more

concerned about new technologies and their effect on privacy, than the group who did not watch the video. Accordingly, it follows that once the participants were educated on various technologies and matters of privacy, they were more likely to express their concern with respect to the consequences of technology on privacy.

Sharing Personal Information

An independent-samples *t*-test revealed a significant difference between groups and their comfort level, in sharing personal information with the government; (t (58) = 2.522, $p < 0.05$). [Question 12e] (see Appendix E, Table 1). This finding suggests that those who did not watch the video were more comfortable in sharing their personal information (i.e., name, address, telephone number, e-mail address, date of birth, or financial information) with the *government*.

A difference was also identified between the group who did not watch the video, and the group who watched the video, and the level of concern regarding personal information held by various institutions; (t (58) = -2.442, $p < 0.05$). The group who viewed the video was more concerned that their personal information, held by various institutions, may be used to execute decisions about them, which may affect their chances of being granted or denied a service. [Question 31] (see Appendix E, Table 1).

Decision-making

There was a strong, statistically significant difference between groups about concern that a decision about their character or personality may be executed solely based on particular personal information (t (58) = -2.855, $p < 0.05$). The group exposed to the video was more concerned that a decision about their character/personality such as trustworthiness and loyalty may be executed, exclusively on the basis of their specific

personal information. This question is important in that it gets to the power of erroneous information affecting life course. For instance, if one is in debt, an employer may decline to hire the individual based on the fact that as a result of their debt situation, that individual is more likely to be influenced by a bribe [Question 32] (see Appendix E, Table 1).

A statistically significant difference was also evident between groups with regards to personal information which is collected by agencies (t (58) = -2.427, $p < 0.05$). The experimental group was more concerned about their information being collected and retained by different agencies or institutions, than the control group. [Question 34] (see Appendix E, Table 1).

Radio Frequency Identification (RFID)

A further significant difference existed between both groups on the subject of Radio Frequency Identification (RFID) chips (t (57) = -2.431, $p < 0.05$). After viewing the video, the experimental group was significantly more concerned that RFID chips may be imbedded in products which they purchased; as they emit radio waves and can track where one takes and stores the item which he/she has purchased. Thus, resulting in more information being inferred about the individual who purchased the item. [Question 44] (see Appendix E, Table 1).

Protection of Personal Information

There was no significant difference between groups regarding whether or not they provide their postal code when requested by a retail store, (X^2 (2, 60) = 3.048, $p = ns$). [Question 11] (see Appendix E, Table 4). As the video could not have made any impact here this is a good indicator that the groups were comparable and adds to the veracity of

the other findings. There was no significant difference between the two groups in experiencing a serious incident where their personal information was used inappropriately or released without their consent (e.g., credit card information), (X^2 (1, 59) = 0.003, $p = ns$). [Question 13] (see Appendix E, Table 3a). Again, this is a welcome finding as the results here are an indicator that the participants in both groups have similar historical experiences regarding incidents of privacy and personal information. Similarly, when both groups were asked to respond to whether or not they shred or destroy documents containing personal information (e.g., credit card offers, insurance and loan applications, bills and credit card receipts), there was no significant difference in their responses, ($X^2 = 3.590$, $p = 0.058$) [Question 14] (see Appendix E, Table 3a). When participants responded to the question regarding whether or not they have ever reviewed an organization's privacy policy, there was again no significant difference between groups ($X^2 = 1.086$, $p = ns$). [Question 15] (see Appendix E, Table 3a).

No significant difference was found between the two groups in their beliefs about whether their personal information (e.g., name, age, address, income, e-mail address etc.) possesses any value to others (e.g., companies, organizations, government, etc.), (X^2 (2, 60) = 3.889, $p = ns$) [Question 17] (see Appendix E, Table 4) which seems to support the idea that consumers are not typically bothered by exchanging their personal data for access to perks or products.

When asked if they have ever given a store incorrect information, when their name, phone number or postal code were requested, in order to protect their personal information or for privacy reasons, no significant difference was exhibited ($X^2 = 0.000$, p

= *ns*). In fact, the results were divided equally – 14 participants from both groups scored "yes" and 16 participants selected "no". [Question 18] (see Appendix E, Table 3a).

Participants were asked whether they have ever inquired with a store, why their personal information (i.e., name, phone number or postal code) is needed. There was no significant difference between groups ($X^2 = 0.077$, $p = ns$). [Question 19] (see Appendix E, Table 3a). Respondents were then asked if they have ever refused to provide their personal information (i.e., name, phone number) to a store. There was no significant difference between the two groups (X^2 (2, 60) = 4.273, $p = ns$) [Question 20] (see Appendix E, Table 4).

Question number 4 asked participants to rate the degree to which they agree or disagree with the following statements using a 7 point scale, where 1 means "strongly disagree", 7 means "strongly agree" and the mid-point 4 means "neither agree nor disagree". The statements are as follows ([*a* to *h*] see Appendix E, Table 8): [Question 4]

(a) I have enough information to know how new technologies might affect my personal privacy.

There was no statistically significant difference between groups (t (58) = 1.359, $p = ns$). The mean value for both groups scored around 4 ("Neither Agree nor Disagree") and 5.

(b) I take adequate precautions to protect my information on social networking sites such as Facebook.

There was no statistically significant difference between groups (t (57) = 1.216, $p = ns$). The mean value for both groups scored between 4 ("Neither Agree nor Disagree") and 5.

(c) Even if my privacy is breached, the consequences are not significant.

An independent-samples *t*-test revealed a strong, statistically significant difference between group 1 and group 2 and the extent to which they are concerned about their privacy being breached and the significance of the consequences of such; (t (58) = 2.812, $p < 0.01$). The results revealed that those who watched the video were much more concerned that if their privacy was breached the consequences would be significant.

(d) I am concerned about personal information becoming public that may be embarrassing to me.

There was no statistically significant difference between groups (t (58) = -0.823, $p = ns$).

(e) I am concerned about the financial risk of online commerce.

There was no statistically significant difference between groups (t (57) = -1.131, $p = ns$).

(f) I am concerned that my friends might end up providing information to others about me through social networking.

The independent-samples *t*-test revealed a strong, statistically significant difference between group 1 and group 2, and the concern that the participants' friends may provide information to others about them, through social networking (t (58) = -3.208, $p < 0.01$). The subjects who viewed the video were significantly more concerned about the possibility that their friends may reveal information to others about them through social networks, than those who did not watch the video.

(g) I am concerned that corporations might end up using information about me that I didn't approve of or know about.

There was also a very statistically significant difference between groups regarding concern that corporations may use information about the participant, that he/she did not approve of or know about; (t (58) = -3.001, $p < 0.01$). The individuals who watched the

video were particularly more concerned than those individuals who only completed the questionnaire.

(h) I am concerned that the government might end up using information about me that I didn't approve of or know about.

Amongst all the statements for question number 4 listed above, participants' concern that the government may use information about them that they did not approve of or know about, displayed the strongest statistically significant difference between group 1 and group 2; (t (58) = -4.139, $p < 0.01$). The experimental group was extremely more concerned than the control group, that the government could use their information without their approval or knowledge.

In question number 27, the subjects were asked if they have ever considered the consequences of sharing personal information with others (i.e., friends, institutions, government, businesses, etc.), to which they exhibited no difference: ($X^2 = 0.000$, $p = 1.000$). In fact, the results from each group were exactly the same – in both groups 1 and 2, 86.7 per cent replied "yes" and 13.3 per cent replied "no" [Question 27] (see Appendix E, Table 3b).

When questioned on whether or not they will employ particular measures to protect their personal information, responses from both groups revealed that no statistical significance exists, ($X^2 = 1.071$, $p = ns$). [Question 40] Furthermore, when the subjects were asked about their concern regarding the possibility of misinformation (i.e., inaccurate/incorrect information) that may be contained in various databases/systems held by institutions, no statistical significance was exhibited, (X^2 (1, 59) = 1.023, $p = ns$). [Question 41] (see Appendix E, Table 3b).

Question number 42 states, “Do you agree with the statement: you have the right to privacy, but not the right to anonymity?” There was no statistical significance, (X^2 (1, 59) = 2.255, $p = ns$) [Question 42] (see Appendix E, Table 3b); however, 30 per cent of the subjects in group 1 selected “yes”, whereas 13.8 per cent of the subjects in group 2 selected “yes”. A segment of the video states this exact sentence, by a non-privacy advocate. Interestingly, there was a decrease in percentage, or less participants from group 2 which replied “yes” to this question. Thus, one may speculate that the video had an impact on those participants. In other words, 86.2 per cent of the subjects in the experimental group (versus 70 per cent in the control group) disagreed with the above noted statement. Therefore, holding an opinion contrary to that held by the non-privacy advocate; and believing instead that one should have both the right to privacy, and the right to anonymity.

Question number 43 asks participants the following: “Do you believe that Facebook uses technology, to encourage or trick its users to disclose more personal information about themselves, than they might otherwise choose to disclose?” Although there was no statistical significance, (X^2 (2, 59) = 5.476, $p = 0.065$) [Question 43] (see Appendix E, Table 4); there was a higher percentage (i.e., of participants) from the experimental group (79.3 per cent) which selected “yes”, versus the control group (70.0 per cent). From the experimental group, 0 per cent of the participants selected “no”, and the remainder (20.7 per cent) selected “Don’t know” (13.3 per cent from the control group selected the latter). Interestingly, it seems that the video influenced the participants’ decision regarding this question, as none of them selected “no”. Therefore, all participants in the experimental group, except 20.7 per cent who selected “Don’t

know", agreed that Facebook uses technology, to encourage or trick its users to disclose more personal information about themselves, than they might otherwise have chosen to disclose. A segment of the video explained how Facebook used biometric technology to recognize individuals in photos which are uploaded to Facebook; thus, most likely accounting for these responses.

Use of Personal Information by Institutions

Question number 22 asked participants what they think stores or organizations do with their personal information. The following list of options was provided, and participants were instructed to select as many as they believed applied: [Question 22] (see Appendix E, Table 13)

- Compile statistics/demographic information on their customers;
- Sell the information/sell it to telemarketers/put you on a mailing list;
- Create mailing/phone lists;
- Marketing/targeted marketing/increase sales;
- Advertising;
- Worries about confidentiality/safety/hacking and fraud;
- To check my identity/credit/fraud protection;
- Conduct market research;
- For contact purposes/keeping track of my points/warranty/discounts;
- Other – please specify;
- Don't know/Refused.

The only statistically significant difference between the control group and experimental group in participants' thoughts regarding what stores or organizations do with their

personal information was "To check my identity/credit/fraud protection" ($X^2 = 6.667$, $p < 0.05$). A total of 33.3% of the respondents from the experimental group, compared to 6.7% from the control group, selected "To check my identity/credit/fraud protection". Despite the experimental group's knowledge acquired from watching the video, it is surprising that most respondents from that group did not select the option that stores/organizations use personal information to compile statistics and demographic information on their customers, or sell the information (e.g., to telemarketers).

Law and Protection of Personal Information

Question number 5 asked participants to rate how important it is to them, to have strong laws protecting Canadians' personal information. There was no significant difference between the two groups, both scored a mean of 6 (control group: 6.03; experimental group: 6.00), on a scale from 1 ("Not at all Important") to 7 ("Extremely Important") [Question 5] (see Appendix E, Table 9). Generally speaking, regardless of their exposure to educational awareness about privacy, all respondents expected a strong legal framework to safeguard privacy.

Open-ended Questions: Control Group

The control group – those not exposed to the condition or video – scored the following, when asked whether they are concerned that some of their information, contained in a database (e.g., Facebook, retail or government databases, etc.), may fall into the wrong hands (e.g., corruption; manipulation or leak of information, etc.). Only 27 of the 30 participants responded to this question; 6 of which were not concerned or slightly concerned, stating that they have nothing to hide or would not share information (e.g., post information on Facebook), if they did not want it to be in the public realm. In

contrast, 21 participants were concerned that some of their information in databases, may fall into the wrong hands; primarily citing concern with regards to internet vulnerabilities such as hacking and stealing personal information from databases; to be used maliciously against the individuals whose information was stolen. Amongst other concerns were the use or selling of one's personal information, to make money; fear of a corrupt government, framing individuals with competing political views; and the unbalanced power of corporations versus individuals, i.e., policies are not strong or powerful enough to protect or support the individual. [Question 35]

Participants were asked how they feel, after they were made aware of the implications involved with regards to privacy and personal information. Six out of 30 participants in the control group did not respond to the question. Half of the group (i.e., 12 individuals – excluding the 6 who did not answer the question) expressed concern; citing the following: they are troubled that information about them on the internet may be used by corporations, to make decisions about their integrity or character; worried that Canada is heading into a "Big Brother" society; one's privacy is not respected and nowadays one has less control over their privacy and personal information. Six individuals felt indifferent about the matter; whereas another 6 felt more educated on the matter and its implications and stated they will modify their behaviour, to protect their privacy and personal information. [Question 36]

Four individuals out of 30, in the control group did not respond to the question regarding whether or not it concerns them that all the personal information they have voluntarily disseminated will never be retrievable (i.e., permanent electronic records). Eight participants indicated that they are not concerned; providing the following reasons:

they choose the information they want to share; releasing very sensitive information only to trusting places; and due to the volume of data available, the likelihood of their information becoming compromised or targeted is unlikely. The other 18 participants stated, they are concerned that their personal information, which they have voluntarily disseminated, is not retrievable and a permanent record. The following explanations were provided: losing control over one's personal information grants more power to corporate and state entities; deleting personal information from social media websites does not actually remove the content from cyberspace or the internet. Other reasons were that one's personal information could be used without the individual's consent; to make decisions against individuals; or could be used to commit fraud. [Question 37]

When the participants in the control group were asked whether they think the information contained about them in a database will affect them in the future, 14 replied they are concerned, because it may affect their life, e.g., future career prospects; fraud or theft of personal information and misuse of personal information. Specific examples which were provided: personal information can dictate future employment, house ownership; and online activity and credit history may also impact one's future. Three participants did not respond to the question. Seven individuals were undecided about the matter, or unsure. A total of 6 subjects were not concerned. [Question 38]

Participants were asked how they feel about institutions using their personal information contained in a database, to make inferences and decisions about them (e.g., granting loans, employment, classify one in a particular group or category, etc.). Only 27 participants in the control group responded to this question. Four individuals were not concerned; one stated that it is necessary and must be done, as it protects the institution.

For example, in trying to obtain a loan, the institution granting the loan needs to know that the individual they are granting the loan to, possesses the means to pay them back. Only one individual was unsure about the matter. All remaining 22 participants were concerned, some which felt that it was unfair and discriminatory; stating that corporations should not be able to discriminate against a person based on their political ideology, sexual orientation, or other personal information. Others felt fearful that certain institutions will use their information against them, to classify them in a specific group and deny them a service; some felt that institutions should not have the right to see one's personal information without their consent; and others felt that it was an invasion of privacy and were uncomfortable or upset regarding the matter. [Question 39]

Open-ended Questions: Experimental Group

Respondents were asked whether they are concerned that some of their information contained in a database (e.g., Facebook, retail or government databases, etc.), may fall into the wrong hands (e.g., due to corruption; manipulation or leak of information, etc.). Of the 30 respondents in the experimental group, only a small minority (n=4) stated that they were not concerned that their information may fall into the wrong hands, maintaining that either they have nothing to hide, or believed that their information holds no value. Contrarily, the large majority of respondents in the experimental group (n=26) were concerned that their information may fall into the wrong hands: the majority of which (n=11) felt that such information can be manipulated and used maliciously. Many provided examples such as identity theft and other crimes such as fraud; denial of service(s) based on collected personal information; breach of trust; exploitation; and misinterpretation of information, which may result in dire and possibly

irreversible consequences. The other main reason participants were concerned contended that such information should be protected and remain private; one specifically stated that individuals need a level of control over their identity, and others even suggested the implementation of stricter privacy laws. Amongst those concerned, other reasons cited were power imbalances (e.g., abuse of power by government); the value of personal information, especially in light of the ease with which such information may be accessed and/or voluntarily provided; vulnerabilities such as hacking databases/systems; and leak of information. [Question 35]

All 30 respondents in the experimental group provided a response regarding how they felt, after they were made aware of the implications involved with regards to privacy and personal information. Only 4 of the subjects felt indifferent towards the matter, after they viewed the video. Nine participants felt scared, uneasy/disturbed and violated. Seven subjects felt more educated and aware of the implications of privacy and personal information; stating that they are now better prepared or equipped to protect their privacy in the future. The remaining 10 participants felt concerned; asserting that they were not aware of the extent to which they are being monitored and the level of surveillance; they felt less secure about providing personal information and helpless, i.e., for instance, feeling that there are not many things one could do to prevent others from obtaining their personal information or invading their privacy; and if so, that it is too late – Facebook and Google already have their information. Also, the negative social implications of disconnecting from social networks was a concern or dilemma. [Question 36]

One of the 30 subjects in the experimental group did not respond to the question regarding whether or not it concerns them, that all the personal information they have

voluntarily disseminated will never be retrievable (i.e., permanent electronic records). Four respondents were not concerned, as they believe such is bound to happen, given technology's evolution (technology or the internet is the future). The remaining 25 respondents were concerned that their voluntarily disseminated personal information is not retrievable and a permanent record. The majority were concerned that their information could be used against them (i.e., including manipulation of information, or using the information to make decisions about the individual, which could affect their future); and that it is not retrievable, which may lead them to have to face the consequences. The argument that people change over time was mentioned; thus, permanent records may not allow for changes, accordingly. Not possessing control or power over one's own personal information was also another reason for concern. [Question 37]

All 30 participants in the experimental group responded to the question regarding whether they think the information contained about them in a database will affect them in the future. A total of 22 subjects stated they are concerned, 11 of which specified that such may affect their future career prospects and life; the remainder (i.e., other 11 subjects) cited the following reasons: control of individuals by reducing their freedom; denial of service (e.g., character judgment); risk of personal information falling into the wrong hands and used against the individual; targeted advertisements. Four subjects were unsure whether their information, captured in a database will affect them in the future; and another 4 did not think their personal information (contained in databases) will affect them in the future. [Question 38]

The 30 respondents in the experimental group were asked how they felt about institutions using their personal information contained in a database, to make inferences and decisions about them (e.g., granting loans, employment, classifying one in a particular group or category, etc.). Only one of the 30 respondents did not provide an answer to the question. Two people were indifferent, and one person was unsure about the matter. Two individuals felt that institutional collection of personal information is necessary, and only one individual was not concerned. The remaining 23 respondents felt concerned about this matter; especially if one's personal information is used to make discriminatory judgements (e.g., denial of service etc.). Many of the respondents felt violated and believed that personal information should be kept personal. Some respondents were concerned about the accuracy of such personal information being held in these databases; and others were of the opinion that personal information should not define a person or be the base of a decision about a person. [Question 39]

The results from questions number 21 and 28 were omitted because participants did not respond to the questions correctly. Question number 21 states: "Why did you refuse to give your personal information or give incorrect information? Please select one of the following." The options listed for this specific question are as follows:

- Unnecessary/they didn't need it;
- Don't trust the store;
- Don't want to be contacted by telemarketers/avoid junk mail/they'll try to sell me something; Personal/private information;
- None of their business;
- Concerned about identity theft/fraud/computer hackers;

- Safety/security issues – unspecified;
- Depends on the situation/will give it on occasion;
- Because I didn't want to/wasn't interested in offer;
- I didn't refuse;
- Other;
- None/no reason;
- Don't know.

Most participants selected more than one option from the list; rather than only one answer, as instructed. Question number 28 asks participants the following: "Please rank the following types of information in the order in which you consider them to be the most personal from 1 – 12 (1 is most personal, 12 is least personal), and are reluctant to share?" The options are as follows: Name, Age, Home address, E-mail address, Employment status, Income, Marital Status, Health history, Criminal history, Credit history, Educational history, Driving record. Once again, most participants incorrectly completed this question. Rather than utilizing each number once, using the scale 1 to 12, several participants instead marked the same number more than once. For example, number 5 was used more than once for each of the 12 listed items. [Questions 21 and 28]

Questions number 2, 10, 13-15, 18-19 are displayed in Table 3a: *Respondents' personal history with privacy* (see Appendix). The results displayed in this table are not statistically significant, with the exception of one (question number 14). The data revealed that no difference exists between either groups (i.e., control and experimental), regarding participants' personal history with privacy; thus, rendering this research study more valid. In other words, since both groups' personal history with privacy is more or

less the same, this provides a strong basis upon which to transfer results from this research study, to the general public.

Chapter Five: Discussion

The main objective of this exploratory study was to empirically test the effect of viewing news content and information about breaches of privacy. In particular, whether exposure to such news stories and information affects awareness or potential precautionary behaviour. As technological advancements in surveillance continue to expand, this thesis aimed to test the malleability of perceptions of privacy among a selection of the university student body. In other words, does increased awareness of surveillance technology and its range of actual and potential uses, affect individuals' concerns about privacy? In order to test this, a video was created to educate participants. A semi-random selection process was used to recruit subjects for the research study. Two groups were formed; an experimental group viewed the video and subsequently completed a questionnaire, whereas a control group only completed the questionnaire (and did not watch the video). It was expected that those participants who viewed the video would become more educated on matters of privacy and existing surveillance technologies and would therefore express a more cautious sensibility towards technological advancements that may compromise their privacy, and would likely want to undertake precautionary measures to protect their privacy and personal information.

Overall, the findings suggest that the educational video did indeed have an impact on the experimental group. The data reveal that as a result of watching the video, the experimental group had elevated awareness about the implications of surveillance technologies, dissemination of personal information, and the pitfalls of not safeguarding privacy leading to a heightened level of concern amongst most respondents. Consequently, the results suggest that building awareness and educating individuals on

privacy and surveillance matters will lead them to take precautionary measures in protecting their privacy and personal information. Although further testing amongst a larger population is required, this exploratory study indicated that educational initiatives aimed at a wider constituency can have a significant impact on public attitudes toward privacy, at least in the short-term.

Findings in Context

The findings presented in this thesis therefore indicate that once people are made aware of the scope and reach of existing surveillance technologies and the negative consequences of voluntarily disseminating personal information and not taking precautions to protect privacy and personal information, individuals' perception of privacy will change. Interestingly, the findings from this research (question number 4.g) mirrored Smith and Lyon's (2013, 190) study of Canadian and American respondents who expressed concern regarding what corporations may do with their information. Subjects from the experimental group were far more concerned than those from the control group that corporations may end up using information about them that they did not approve of or know about. According to the same study, knowledge about RFID and biometric technology remain poor and on the decline since 2006. This thesis confirms these results as 21 out of 30 respondents (from the control group) had no knowledge of RFID technology, and 23 out of 30 respondents (from the control group) were still unaware of biometric technologies (see questions number 7 and 8).

In Smith and Lyon's study (2013, 190), younger people between the age of 18 and 34 years felt they had more control over what happens to their personal information than older people (35 to 54 years old). In my research study, 66.7% of participants from the

control group believed they possessed an adequate level of control over their personal information (see question number 25). In contrast, there was a significant difference between groups: only 33.3% of respondents in the experimental group felt they had an adequate level of control over their personal information. It appears that the more knowledgeable (or experienced) we become with surveillance technologies and their range of actual and potential uses, the less confident we are believing that we have an adequate level of control over this information. In comparing findings from 2006 and 2012, there was a notable increase with participants purposefully providing false information about themselves to marketers – from 20% to 43% in Canada. In my research study, 46.67% from both groups disclosed that they have given a store incorrect information when asked for their name, phone number or postal code to protect their personal information, or for privacy reasons (see question number 18). These findings suggest that there may be a greater awareness amongst university students, regarding the need to protect personal information. Nonetheless, the numbers are still less than 50%, indicating that education is lacking within this field and creating awareness is necessary.

The Office of the Privacy Commissioner (OPC) found that 60% of Canadians believed that they had less protection over their personal information in their daily lives than they did 10 years ago (OPC 2011). In this thesis, respondents scored a mean value of 3 – *Neither good nor* bad – in both groups, when asked to rate how well they believe they are doing in protecting the privacy of their personal information, on a daily basis (see question number 3). These findings are alarming, as the latter demonstrates a lack of concern on the part of the subjects who participated in the study, and their regard for protecting their privacy/personal information. Additionally, the OPC's findings in 2011,

to a degree, support the possibility that nowadays more Canadians believe they have less protection over their personal information than they once did. About 45% of Canadians who participated in the OPC's research study and used social networking sites, declared their privacy concerns surrounding social networking sites. In my research study, 80.0% of respondents – both groups combined – stated that they used Facebook or other social networking websites, and employed the privacy settings to set restrictions to their profile (see question number 16). These findings indicate that most participants in my research study utilize Facebook. When participants were asked whether they believe Facebook uses technology to encourage or trick its users to disclose more personal information about themselves, most participants from both the control and experimental group agreed (control group [70.0%]; experimental group [79.3%]) (see question number 43). If participants are aware of these tactics why do they not seem to be concerned? Why do they continue to use Facebook? If most individuals provided incorrect or false information about themselves in creating their Facebook account, then perhaps it follows that they are taking necessary precautions to protect their personal information. However, based on the findings of my research study, it is likely that many people actually provide their actual personal information, rather than fabricating the information. Evidently, there is a lack of awareness about the range of existing surveillance technologies and its detrimental effect on privacy.

In 2011, the OPC's study revealed that only 7% of Canadians read privacy policies. In contrast to my research study, 63.3% of respondents from the control group and 50.0% of the experimental group maintained that they have reviewed an organization's privacy policy (see question number 15). Whether this was a common or

one-off practice was not explored. Further research is required, to identify if Canadians read privacy policies when they surrender their personal information.

As we have seen in Chapter One, the concept of privacy and its definition is widely contested amongst academics. Goold (2002, 22) believes that privacy is the liberty to choose how to respond to the demands of others, while maintaining a degree of control over the way in which one presents himself/herself to the world. He asserts that privacy rights should be protected, as they are essential for the maintenance of personal autonomy, and also enable individuals to preserve different and valuable social relationships. Contrarily, Stalder argues that privacy is a vague concept, and contends that it cannot be applied in the public realm, as it is difficult to avoid entering into relationships that produce electronic, personal data. Stalder maintains that privacy is by definition personal because every individual has a different notion about what constitutes privacy. Consequently, it is difficult to come to a consensus as to what are the legitimate boundaries of the privacy bubble. Stalder raises an interesting paradox inherent in modern society: most individuals are concerned about privacy; however, in practise most do little to protect it. (2002, 121-122). Although Stalder's argument seems plausible, one must question why it is the case that, as Stalder maintains, many people may be concerned about privacy, yet few do very little to protect it? As my research study demonstrates, most individuals are unaware of existing surveillance technologies which are applied on a daily basis, to glean personal information from people; individuals do not possess sufficient knowledge and/or do not seem to be well versed regarding the means through which they can protect their privacy and personal information.

In this study, when participants were asked to select from a list of options, what the term "privacy" meant to them, there was no statistically significant difference between the control and experimental groups in associating the listed terms with privacy (see question number 1). Within both the control group and the experimental group, the option which was selected the most was "Confidentiality of personal information" (see Table number 2). The findings specific to this question revealed that no differences existed between the control and experimental group; thus, indicative of a general understanding of the connection to privacy and the terms exists, regardless whether one is exposed to the video or not. Stalder's argument that privacy is by definition personal, is supported by my research findings, as each participant selected various combinations of what the term privacy meant to them; despite the general understanding of what the term privacy entails, and the high scoring of "Confidentiality of personal information". In this research study, the power of media (i.e., impact of the video) was key in determining whether creating awareness of surveillance technologies affected or influenced people's way of thinking about privacy. The findings indicate that the video did indeed affect participants' perception of privacy (see question number 33).

The results from my research study indicate that most individuals value their privacy; but even more so after having watched the video which created enhanced awareness amongst its viewers on surveillance and privacy. The results also bring to light the participants' lack of knowledge about existing surveillance technologies and the way in which they are used to collect each individual's personal information as well as poor knowledge of the risks associated with dissemination of personal information. After the participants were exposed to the video, most participants in the experimental group (26

out of 30) were influenced and expressed feelings of uneasiness towards their privacy. Others admitted they were not aware of the extent to which they were being monitored or surveilled, and felt less secure about providing their personal information. Additionally, several participants declared they felt more educated about the implications regarding privacy and personal information, and consequently felt better equipped to make an effort in protecting their privacy in the future. The control group (18 out of 24) also expressed very similar concerns as the experimental group; participants felt troubled and stated that our society is becoming more like a Big Brother society, and many affirmed they would modify their behaviour in order to protect their privacy and personal information (see question number 36). More than three quarters of the subjects from the control group (90.0%), and nearly all the subjects from the experimental group who watched the video (96.7%), stated that they will employ particular measures in the future to protect their personal information (see question number 40).

Anonymity

Penney argues that privacy in the form of anonymity may encourage individuals to participate in activities that they would otherwise not engage in (Penney 2007, 493). In a segment of the video, a representative of a company that collects individuals' personal information on a daily basis made the following statement: "you have the right to privacy, but not the right to anonymity." Subjects in my research study were asked whether they agreed with this statement; from the control group only 30.0% agreed, and even fewer participants from the experimental group (13.8%) agreed. (see question number 42). The importance of both privacy and anonymity are evident in my research study's findings, and highlighted in Penney's argument. It is crucial that both one's privacy and anonymity

are maintained so as to encourage people to participate in various activities including donating to specific foundations, completing surveys, and inquiring about personal matters (e.g., calling an information line to seek assistance, help or advice), etc. If individuals are restricted from being anonymous entities, there is a greater chance that they may withdraw from society or choose to remain excluded from certain activities or services. For example, a teenager who is contemplating suicide and in desperate need of help, may call a helpline which caters to people in distress. However, should the caller's identity be required (i.e., anonymity is not an option), the distressed or troubled individual may be deterred from calling and seeking help or advice; consequently leading to his demise. Individuals should possess the right to privacy and anonymity. While it is understood that many organizations require individuals' personal information, in order to enter into a contract or provide services/items to protect themselves, it does not follow that every individual should be robbed of their privacy and anonymity. In other words, we need some balance – privacy and anonymity ought to coexist in a modern surveillance society despite technological advancements and institutional or corporate demands for personal information.

Bennett contends that the public's interest is in controlling excessive surveillance; rather than private interests to protect privacy (Bennett 2011, 490). One may argue however, that the former and latter are one and the same; or both are equally important in order to prevent the erosion of privacy. Consider for instance the following: each institution possesses personal information in a database and people disseminate their personal information on the internet via social networks, electronic mail, online transactions etc. Presuming this information is not being surveilled and is instead simply

stored in various databases, the possibility that this information may be compromised at any given point in time, is always present. In other words, the fact that our information is permanently stored in numerous databases or in cyberspace, and the fact that it is irretrievable poses a risk to our privacy – a breach could occur at any given moment. The spectre of biographical violation hangs over our existence.

Responsibility and Awareness

Earlier we discussed how Clarke (1994) offers the notion of the "data double" or digital persona. An identity that is created from coded categories, that is extracted from individuals' daily transactions that may open or close doors of opportunity and access (Lyon 2003, 27). The findings revealed that most participants had no previous knowledge about the concept of a data double (96.7% of the control group – see question number 8). Furthermore, participants from both groups expressed concern about their personal information being held by various institutions (see questions number 31 [mean higher than 5] and 32 [mean higher than 4]). Thus, by creating awareness of the implications surrounding the dissemination of personal information and the lack of privacy protection, it influences participants to change their perception of privacy and consider taking the appropriate measures to safeguard their personal information.

In this regard, Gilliom (2011, 502-503) has questioned whether most individuals are aware of the fact that they live in a surveillance-intensive society. As we have already noted, for Gilliom (2011) people do not seem conscious of the fact that the contemporary society is saturated by surveillance. Supporting this argument are the findings from my research study: the control group was less informed than the experimental group on various matters relating to privacy and surveillance. There is a great lack of awareness

amongst participants, which was evident in both groups. We have already seen that when Gilliom (2011, 502-503) provides his own example, informing his students that their cellular phone is a *de facto* location and interaction monitor, and that every credit card transaction records a merchant code, revealing the nature of their business, his students were genuinely surprised. Gilliom (2011, 502-503) suggests that individuals would better 'see' the growing surveillance problem, if it were presented to them in the form of social control. Although the video which was presented to the experimental group did not necessarily discuss surveillance as a generalized means of social control, it was apparent that most participants (14 out of 27 from the control group; 22 out of 30 from the experimental group), were concerned that their personal information held in a database may affect them in the future. Participants from the control group cited their concern about future career prospects; fraud or theft of personal information and misuse of personal information; stating that personal information can dictate future employment, and house ownership; and online activity and credit history may impact one's future. Subjects from the experimental group expressed concerns about future career prospects, life course, the control of individuals by reducing freedom, denial of service (e.g., character judgment), risk of personal information falling into the wrong hands, and even targeted advertisements (see question number 38). The findings from my research study reinforce the fact that even when surveillance is presented through a framework other than social control, i.e., value of personal information and privacy, subjects are still receptive, and their perceptions are nevertheless impacted.

Controlling excessive surveillance, whether undertaken by companies or institutions is crucial. However, individuals to an extent also possess responsibility and

control over their personal information. Therefore, both the people and surveillance society play a role in maintaining or upholding the concept of privacy and what it entails. In my research study, participants expressed concern about voluntarily disseminated personal information being irretrievable and permanently stored because of technological advancements. Eighteen subjects out of 26 from the control group were troubled that they have lost control over their personal information. Others were concerned about the misuse of their information including manipulation, fraud, and poor decision-making. A total of 25 out of 29 subjects from the experimental group were worried that they no longer possess control over their information, and that it may be used against them. (see question number 37).

Gandy (2009) claims that there is no invasion of privacy through the collection of personal information, rather it is the classification and assessment of the information which creates a power imbalance – discrimination is based on classes of people. Although Gandy raises a valid point at the aggregate level, it may be argued that invasion of privacy nonetheless also exists through collection of personal information, regardless of the process of classifying individuals. The mere fact that one's personal information is contained in numerous databases and possessed by various institutions, is sufficient to invade one's privacy. Even if an institution does nothing with one's personal information (i.e., execute decisions and grant or deny services), the fact that the individual's information is not retrievable and no longer in their possession or control, may be considered an invasion of an individual's privacy. An action does not necessarily have to be taken based on one's personal information for it to be considered an invasion of privacy. The simple fact that an individual is no longer the owner of his/her personal

information may itself constitute an invasion of privacy. Additionally, identity theft or fraud is another example of how collection of personal information may lead to the invasion of one's privacy. There is no question that social control may be a consequence of the collection of people's personal information but a power imbalance is created as soon as one relinquishes some or any of their personal information to another entity regardless of what decisions follow. Subjects from both the control and experiment group were concerned about who views, or has access to their personal information (see question number 30).

Lyon (2009, 1) defines surveillance as any focused attention to personal details for the purpose of influence, management or control. He argues that agencies process personal data in order to calculate risks or predict opportunities. The use of searchable databases serves to categorize and profile individuals. The findings of this thesis reveal a variety of participants' concerns that reflect the developments identified by Lyon. Twenty two out of 27 participants from the control group stated that it was unfair and discriminatory for institutions to use one's personal information stored in a database, to make inferences and decisions about individuals. Not surprisingly, they felt that corporations should not be able to discriminate against a person based on their political ideology, sexual orientation, or other personal information. Other participants were fearful that certain institutions would use their information against them, to classify them in a specific group and deny them a service. They believed that institutions should not have the right to see one's personal information without their consent, as it is an invasion of privacy. From the experimental group, 23 out of 29 respondents were concerned that one's personal information may be used to make discriminatory judgements (e.g., denial

of service etc.). Many of the respondents felt violated and believed that personal information should be kept personal. Others were concerned about the accuracy of their personal information held in databases, and were of the opinion that personal information should not define a person or be the base of a decision about a person. (see question number 39). If Lyon's argument that the collection of personal data gives institutions unchecked power to execute decisions about individuals then it follows that once participants were introduced to the fact that this is indeed their reality, their perception of what privacy means and its importance changed. Thus, creating awareness and explaining how the value of one's personal information may be used against an individual increases participants' chances of reconsidering which institutions they will divulge their personal information to in the future.

Limitations of this Study

The goal of this exploratory study was, at least empirically, relatively modest yet the political implications of this research are far more important. For that reason alone it is worth considering the limitations of this thesis in terms of structure and execution. In hindsight, the questionnaire would have benefitted from a *Comments* section to solicit feedback from participants. A follow-up interview may have proved useful in solidifying the findings. While we have a good sense of the immediate effects of exposure to information about privacy and surveillance we do not know how long these changes in sentiment might last. Faced with the prospect of having to decide on whether to 'opt-out' of the lure of social networking, consumption on credit, or even surrendering information for access to perks and products, participant may have felt that participation was worth the risk, or that they had little choice. It would be interesting to see how respondents

made sense of this tension and whether attitudinal differences between groups waned over time. In this regard, future research studies that track awareness and precautionary measures against breaches of privacy ought to be longitudinal, in order to determine whether participants indeed followed through with their decision or desire of employing measures to protect their personal information.

The video was about 26 minutes in duration. If the video was longer in duration would it have been more impactful on the participants? Does more information, more news stories of breaches of privacy make for sharper attitudinal changes? Is there a point of diminishing returns? What about changes to the specific content of the video? For example, cyber crime, identity theft or fraud, and the relative ease with which computers or cellular phones can be hacked when using an open WiFi network may have had a more impactful story not covered in the video. A variety of video content and length would have made this thesis unwieldy but it cannot go unsaid that the specific content and duration of the video intervention is a significant consideration for future research.

A larger sample of participants would also have been useful. The recruitment of non-university students may have produced different results. A more diverse sampling of the Canadian population could have created more generalizable results. The setting where the research study was conducted was also not ideal: the subjects were recruited and participated in the hallways of Carleton University which are high traffic areas likely creating distractions that may have influenced the results. A different, perhaps more quiet or intimate setting with fewer distractions may have produced stronger statistical results by intensifying the exposure to the video content. The questionnaire was also quite

lengthy (44 questions) and may have contributed to participants' losing interest. Consequently, some questions were overlooked and unanswered, possibly for that reason. There may have been a selection bias whilst recruiting participants for this research study, i.e., with regards to participants' time commitment. At the beginning of the recruitment process, individuals had the choice to participate by either only completing the questionnaire, or viewing the video and completing the questionnaire (lengthier time requirement). These concerns, however, are ameliorated by the fact that there were no statistically significant differences between the experimental and control groups in terms of their historical experiences regarding incidents of privacy and personal information (see Appendix E: Question 10, Table 3a; Question 11, Table 4; Question 13, Table 3a; Question 14, Table 3a; Question 29, Table 1).

Chapter Six: Conclusion

The two key findings emanating from this study are, first, that a majority of university students who participated had poor knowledge of specific technologies used to conduct surveillance and collect personal information. Most subjects were unfamiliar with technologies such as biometrics and RFID (Radio Frequency Identification). Second, this research study also found strong evidence that educating individuals about privacy and surveillance technologies leads to statistically significant changes in perception of privacy. In other words, creating awareness of the various existing surveillance technologies (including Closed Circuit Television cameras, use of social media, biometrics [e.g., facial and iris recognition software], as well as RFID chips; in addition to the consequences arising from disseminating personal information unnecessarily without regard for privacy) and the range of their actual and potential uses, results in elevated concerns about privacy.

Only after viewing the video did participants acquire sufficient knowledge and understanding of the implications of inaction towards protecting their privacy. There is therefore a pressing need to educate Canadians about existing surveillance technologies employed to glean personal information about them that affects their privacy. The video, which the experimental group viewed, led participants to become very concerned about the lack of control they possess over their personal information. The majority of the experimental group came to believe that it was not possible to maintain a degree of control over their personal information while the less informed control group believed the opposite. Participants who viewed the video were far more concerned with the impact of

surveillance technology and new emerging technologies on their privacy than the group that did not watch the video.

The findings from this research study contribute to the existing academic literature on surveillance and privacy by providing empirical evidence that attitudes toward privacy are malleable, through exposure to news and information about the pitfalls and implication of sharing personal information. There is a great need to educate society about the negative implications of voluntarily and unnecessarily disseminating personal information. Individuals are largely unaware of how their actions and inactions concerning the management of their personal information affects their future prospects. Our society is moving towards increasing transparency. Our movements and activities are endlessly monitored, recorded and stored. Privacy is being eroded and individuals are sleepwalking into a surveillance society where personal information will already always be in possession of governments, institutions, and agencies. We might no longer enjoy the freedom of choosing whether or not to share our information. Rather, we would represent nothing more than data points in the surveillant assemblage.

Future research should focus not only on changing attitudes toward privacy but aim to map how privacy is understood by the public. It is not enough to establish that knowledge of the surveillance technologies changes attitudes. It is also important to map the boundaries of privacy. This is not just a theoretical and legal question. It is also empirical. Canadians engage with a plethora of surveillance mechanisms. These various technological tools should be explored including their frequency and the reasons for their use.

With the rapid rate at which technology is advancing, infiltrating our lives, creating dependency, it is crucial that we foster an informed discussion. Sometimes we cannot see the forest for the trees. We are so wrapped up in the use and participation in surveillance technologies that we no longer see them. What this exploratory study has demonstrated is that it is indeed still possible to see the forest. Awareness is the first step. If Canadians are informed and educated about the means through which surveillance technology is utilized to collect their personal information then perhaps it is still possible for our personal information to remain personal. Or, at least we ought to possess some degree of control over our own information. If we do not become educated about how surveillance technology is used to monitor our activities and behaviour then the idea of privacy will fade from social life.

References

Adams, A. (2015). 50 Inspirational Quotes on Education. Retrieved from http://www .slideshare.net/mobile/EcourseReviews/famous-education-quotes

Anderson, M. (2009, August). Biometrics data is vulnerable, warn experts. *IEEE Spectrum.* Retrieved from http://staging.spectrum.ieee.org/telecom/security /biometrics-data-is-vulnerable-warn-experts

Australian Press Council. (2004, February). Surveillance: an interim report. Submission to the New South Wales Law Reform Commission. Report 98. Retrieved from http: //www.lawreform.lawlink.nsw.gov.au/agdbasev7wr/lrc/documents/pdf/report_98

Bennett, C. J. (2011). In defence of privacy: The concept and the regime. *Surveillance & Society*, 8(4), 485-496.

Brosnahan, M. (2012, December 28). Store video cameras failing to comply with privacy laws. *CBC News*. Retrieved from http://www.cbc.ca/news/canada/store-video -cameras-failing-to-comply-with-privacy-laws-1.1189399

Clarke, R. (1994). The digital persona and its application to data surveillance. Retrieved from http://rogerclarke.com/DV/DigPersona.html

Clarke, R. (2006). 'What's privacy'? Retrieved from http://www.rogerclarke.com/DV /Privacy.html_2006

Clarke, R. (2009). Introduction to dataveillance and information privacy, and definitions of Terms. Retrieved from http://www.rogerclarke.com/DV/Intro.html#DV

Clement, A., Ferenbok, J., Dehghan, R., Kaminker, L., & Kanev, S. (2012). Private sector video surveillance in Toronto: Not privacy compliant! In *Proceedings of the 2012*

iConference, 354-362. doi: 10.1145/2132176.2132222

Deisman, W., Derby, P., Doyle, A., Leman-Langlois, S., Lippert, R., Lyon, D., . . . Whitson, J. (2009). A report on camera surveillance in Canada: Part one – Surveillance camera awareness network. Retrieved from http://www.sscqueens .org/sites/default/files/SCAN_Report_Phase1_Final_Jan_30_2009.pdf

Deleuze, G. & Guattari, F. (1987). *A thousand plateaus*. Minneapolis: University of Minnesota Press.

DesMarais, C. (2012, January). Facebook timeline looms: What you need to know. *PCWorld*. Retrieved from http://www.pcworld.com/article/248925/facebook _timeline_looms_what _you_need_to_know.html

Ditton, J. (2000). Crime and the city: Public attitudes towards open-street CCTV in Glasgow. *British Journal of Criminology*, 40(4), 692-709.

European Commission. (2011). Special Eurobarometer 359: Attitudes on data protection and electronic identity in the European Union. Retrieved from ec.europa.eu/public _opinion/archives/ebs/ebs_359_en.pdf

Feldman, D. (1994) Secrecy, dignity or autonomy? Views of privacy as a civil liberty. *Current Legal Problems*, 47(2), 41-59. doi: 10.1093/clp/47.Part_2.41

Forbes. (2014, April). Lyne, J. Heartbeat Heartbleed Bug breaks worldwide internet security again (and Yahoo). Retrieved from http://www.forbes.com/sitea/jameslyne /2014/04/08/heartbeat-heartbleed-bug-breaks-worldwide-internet-security-again-and-yahoo

Fried, C. (1970). Privacy. *Yale Law Journal*, 77, 475-793.

Gandy, O. H. (2009). *Coming to terms with chance: Engaging rational discrimination and cumulative disadvantage*. Farnham, Surry: Ashgate Publishing.

Gavison, R. (1980). Privacy and the Limits of the Law. *Yale Law Journal*, 89, 421-471.

Gilliom, J. (2011). A Response to Bennett's 'In Defence of Privacy'. *Surveillance & Society* 8(4), 500-504. Retrieved from http://www.surveillance-and-society.org/ojs /index.php/journal/article/view/privacy_response2

Goold, B. J. (2002). Privacy rights and public spaces: CCTV and the problem of the 'Unobservable Observer'. *Criminal Justice Ethics*, Winter/Spring, 21(1), 21-27. doi: 10.1080/0731129X.2002.9992113

Gordon, D. R. (1987). The electronic panopticon: A case study of the development of the national criminal records system. *Politics & Society*, 15(4), 483-511. doi: 10.1177 /003232928701500404

Gray, M. (2003). Urban surveillance and panopticism: Will we recognize the facial recognition society? *Surveillance & Society*, 1(3), 314-330. Retrieved from http://www.surveillance-and-society.org/articles1(3)/facial.pdf

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of Sociology*, 51(4), 605-622. doi: 10.1080/00071310020015280

Haggerty, K. D., & Ericson, R. V. (2001). Policing the risk society. In *Summary and Conclusions* (pp. 448-451). Retrieved from http://books.google.ca/books?hl=en&lr =&id=3XSXgTlx0V8C&oi=fnd&pg=PR11&dq=2001+and+ericson+and+haggerty +policing+the+risk+society&ots=1x40kfEeUc&sig=xz_UkzFRnHBYDpa2LwbbwOU Upi8#v=onepage&q=2001%20and%20ericson%20and%20haggerty%20policing%20 the%20risk%20society&f=false (Original work published 1997)

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

Haight, I. M. (2007). Creative Commons. [Abstract]. Retrieved from http://www.ischool.utexas.edu/~imhaight/projects/surveillant_assemblage.html

Harris, S. J. (1999). Thinkexist Quotations. Retrieved from http://www.thinkexist.com /quotations/technology/2.html

Heckle, R., Patrick, A., & Ozok, A. (2007). Perception and acceptance of fingerprint biometric technology. *Proceedings of the 3rd symposium on Usable privacy and security,* Pittsburgh, PA, USA, 153-154. doi: 10.1145/1280680.1280704

House of Lords. (2009). Surveillance: Citizens and the State. 1, 105. Retrieved from http://www.publications.parliament.uk/pa/Id200809/Idselect/Idconst/18/18.pdf

Idanan, J. (2009) Literature review on face recognition system. Retrieved from http: //ivythesis.typepad.com/term_paper_topics/2009/10/literature-review-on-face -recognition-system.html

Koskela, H. (2002). Video surveillance, gender, and the safety of public urban space: 'Peeping Tom' goes high tech? *Urban Geography*, 23(3), 257-278.

Lawson, P. (2005). Techniques of consumer surveillance and approaches to their regulation in Canada and the USA. Retrieved from http://www.idtrail.org/files /Techniques%20of%20Consumer%20Surveillance%20w%20footnotes.pdf

Ligaya, A. (2013, February). CBC News. How much data privacy can you expect to have? Very little, experts say, given technological advancements and lagging privacy laws. Retrieved from http://www.cbc.ca/news/technology/how-much-data-privacy-can -you-expect-to-have-1.1307856

London Evening Standard (2009, March). George Orwell, Big Brother is watching your house. Retrieved from http://www.thisislondon.co.uk/news/article-23391081-george-orwell-big-brother-is-watching-your-house.do

Lyon, D. (1994). *The electronic eye: The rise of surveillance society*. Minneapolis: University of Minnesota Press.

Lyon, D. (2002). Surveillance studies: Understanding visibility, mobility and the phenetic fix. *Surveillance & Society*, 1(1), 1-7.

Lyon, D. (2003). Fear, surveillance, and consumption. *The Hedgehog Review*, 5(3), 81-95.

Lyon, D. (2003). National ID card systems in public opinion: An international survey. Retrieved from http://www.sscqueens.org/node/79/#lyon

Lyon, D. (ed.). (2003). *Surveillance as social sorting*. London: Routledge.

Lyon, D. (2004). Identity cards: Social sorting by database. Oxford Internet Institute, Internet Issue Brief No. 3. Retrieved from http://ssrn.com/abstract=1325259

Lyon, D. (2009). *Surveillance, power and everyday life*. The Oxford Handbook of information and Communication Technologies pp. 1-37. Retrieved from http://www.sscqueens.org/sites/default/files/oxford_handbook.pdf

Mathiesen, T. (1997). The viewer society: Michel Foucault's 'Panopticon' revisited. *Theoretical Criminology*, 1(2), 215-234.

Monahan, T. (2010). *Surveillance in the time of insecurity*. New Brunswick, NJ: Rutgers University Press.

Neocleous, M. (2007). Security, commodity, fetishism. *Critique*, 35(3), 339-355.

Norris, C. & Armstrong, G. (1999). *The maximum surveillance society: The rise of*

CCTV. Berg, Oxford.

Office of the Privacy Commissioner of Canada (OPC). (2011). 2011 Canadians and privacy Survey: Final report. Retrieved from http://www.priv.gc.ca/information/por-rop/2011/por_2011_01_e.asp

OnStar. (2009). OnStar: Overview. Retrieved from http://www.gm.ca/gm/english/shopping/accessories/onstar

Parliamentary (2009) Surveillance: Citizens and the State. Retrieved from http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1805.htm

Penney, S. (2007). Reasonable expectations of privacy and novel search technologies: An economic approach. *Journal of Criminal Law & Criminology*, 97(2) 477-529.

Pilieci, V. (2010, August). Ottawa Citizen. World is losing grip on privacy: Watchdog. Retrieved from http://www.ottawacitizen.com/story_print.html?id=3413212&sponsor=

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

Rigakos, G. S. (2008). *Nightclub: Bouncers, risk, and the spectacle of consumption*. McGill-Queen's University Press, Montreal & Kingston.

Rule, J., McAdam, D., Stearns, L., & Uglow, D. (1980). *The Politics of privacy: Planning for personal data systems as powerful technologies*. New York: Elsevier.

Saetnan, A. R., Dahl, J. Y., & Lomell, H. M. (2004). Views from under surveillance: Public opinion in a closely watched area in Oslo. Retrieved from http://www.urbaneye.net/results/ue_wp12.pdf

Sanchez, A. (2009). The Facebook frenzy: Resistance-through-distance and resistance-

through-persistence in the societied network. *Surveillance & Society*, 6(3), 275- 293.

Sartori, G. (1970). Concept misinformation in comparative politics. *American Political Science Review*, 64, 1033-1053.

Schneier, B. (1999). Biometrics: Uses and abuses. Retrieved from http://www.schneier .com/essay-019.html

Schneier, B. (2008). *Schneier on Security*. Indiana: Wiley Publishing.

Seven News. (2014, April). Aussie sites affected by Heartbleed Bug. Retrieved from https://au.news.yahoo.com/technology/a/22661514/aussie-sites-affected-by -heartbleed-bug/

Smith, E. & Lyon, D. (2013). Comparison of survey findings from Canada and the USA on surveillance and privacy from 2006 and 2012. *Surveillance & Society*, 11(1/2), 190-203.

Solove, D. (2008). *Understanding privacy*. Cambridge: Harvard University Press.

Spitzer, S. (1987). Security and control in capitalist societies: The fetishism of security and the secret thereof. In J. Lowman & R. J. Menzies & T. S. Palys (Eds.), *Transcarceration: Essays in the Sociology of Social Control* (pp. 43-58). Aldershot: Gower.

Stalder, F. (2002). Privacy is not the antidote to surveillance. *Surveillance & Society*, 1(1), 120-124.

Steeves, V. (2008). Reclaiming the social value of privacy. In I. Kerr, C. Lucock, & V. Steeves (Eds.), *Lessons from the identity trail: Anonymity, privacy, and identity in a networked society* (pp. 193-208). New York: Oxford University Press.

Surette, R. (2005). The thinking eye: Pros and cons of second generation CCTV surveillance systems. *Policing: An International Journal of Police Strategies & Management*, 28(1), 152-173.

The Economist. (2008, December 18). The way the brain buys: The science of shopping. Retrieved from http://www.economist.com/node/12792420.

The Economist. (2013, November 16). Briefing ubiquitous cameras: The people's panopticon, 22, 27-29.

Thomas, K. (2009). School begins using biometric facial recognition. Retrieved from http://rinf.com/alt-news/surveillance-big-brother/school-begins-using-biometric-facial-recognition/5282/

Travis, A. (2009). Lords: Rise of CCTV is threat to freedom. Retrieved from http://www .guardian.co.uk/uk

Westin, A. (1970). *Privacy and freedom*. New York: Atheneum.

Wilson, D. (2007). Australian biometrics and global surveillance. *International Criminal Justice Review*, 17(3), 207-219.

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

Zwick, D. (2009). Manufacturing consumers: The database as new means of production. *Journal of Consumer Culture*, 9(2), 221-247.

Appendix A: Glossary of Key Terms

The following are definitions of terms which will be used in the thesis:

Data double: The data double emanates from the theory of the "surveillant assemblage", whereby the body becomes reduced to pure information. A great deal of surveillance is directed towards the human body. The observed body is broken down by being abstracted from its territorial setting, and then reassembled in different settings through a series of data flows; resulting in a decorporealized body; a 'data double' of pure virtuality. (Haggerty & Ericson 2000, 611, 613).

Dataveillance or Data surveillance: The term dataveillance or data surveillance is defined as "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons" (Clarke 2009). Dataveillance does not monitor the individual, but merely the shadow that the person casts in data.

Visual surveillance: Entails the surveillance of individuals; utilizing instruments such as closed circuit televisions and facial recognition software, for the purpose of monitoring and collecting information.

Informational or **textual surveillance** (equivalent of the term "dataveillance"): Represents the collection and surveillance of personal data; not derived from nor pertaining to visual surveillance. For instance, the collection and monitoring of personal information contained in various databases (e.g., financial information, name, place and date of birth, race, home address, telephone number, social insurance number, occupation, contacts, criminal record, etc.).

Digital persona: The term digital persona reflects the model of an individual's public personality based on data, which is maintained by transactions; and is also used as a proxy for the individual. (Clarke 2009).

Social sorting: The definition of social sorting is the process of exclusion and inclusion; the discrimination between different populations through modes of classification such as ethnicity and religion (Wilson 2007, 213; Lyon 2004, 1). In considering surveillance as social sorting, is to focus on the social and economic categories and the computer codes by which personal data is organized, with a view to influencing and managing people and populations (Lyon 2003, 2).

Phenetic fix: Derived from the term 'social sorting' is the concept of the phenetic fix, which acts to capture personal data triggered by human bodies and uses these abstractions to place individuals in new social classes of income, attributes, habits, preferences, or offences; in order to manage or control them (Lyon 2002, 3).

Appendix B: Questionnaire

Questionnaire

Please Note:** ***Personal Information refers to any information about an individual's identity (e.g., name, age, address, e-mail address, employment status, income, health history, etc.).

1. Which of the following do you think of when you hear the term *privacy?* Please check as many as applicable from the following list.
   - ☐ Confidentiality of personal information (general)
   - ☐ Secrecy/others not knowing your personal information
   - ☐ Security/protection/encryption/passwords
   - ☐ Home/family/bedroom
   - ☐ Being left alone/no solicitation/seclusion
   - ☐ Invasion/lack of privacy
   - ☐ Confidentiality of your personal information (companies)
   - ☐ Confidentiality of your personal information (Internet)
   - ☐ Tracked by government
   - ☐ Freedom/Non-interference/Anonymity
   - ☐ Other – please specify

2. Do you take any measures or precautions to protect your personal information?
   By personal information, we mean any information about an individual's identity, ranging from name, age and address to health history, employment status and income.
   - ☐ Yes
   - ☐ No

	Very Poor	**Poor**	**Neither good nor bad**	**Good**	**Very good**
3. In your day to day life, how good of a job would you say you are doing to protect the privacy of your own personal information.	○	○	○	○	○

4. Please rate the degree to which you agree or disagree with the following statements using a 7 point scale where 1 means you strongly disagree, 7 means you strongly agree and the mid-point 4 means you neither agree nor disagree.

	Strongly Disagree			**Neither Agree nor Disagree**			**Strongly Agree**
	1	**2**	**3**	**4**	**5**	**6**	**7**
(a) I have enough information to know how new technologies might affect my personal privacy	○	○	○	○	○	○	○
(b) I take adequate precautions to protect my information on social networking sites such as Facebook	○	○	○	○	○	○	○
(c) Even if my privacy is breached, the consequences are not significant	○	○	○	○	○	○	○
(d) I am concerned about personal information becoming public that may be embarrassing to me	○	○	○	○	○	○	○
(e) I am concerned about the financial risk of online commerce	○	○	○	○	○	○	○
(f) I am concerned that my friends might end up providing information to others about me through social networking	○	○	○	○	○	○	○
(g) I am concerned that corporations might end up using information about me that I didn't approve of or know about	○	○	○	○	○	○	○

(h) I am concerned that the government might end up using information about me that I didn't approve of or know about	○	○	○	○	○	○	○

	Not at all Important 1	2	3	Somewhat Important 4	5	6	Extremely Important 7
5. How important is it to you personally to have strong laws to protect Canadians' personal information?	○	○	○	○	○	○	○

6. Are there any new technologies that you are particularly concerned about with respect to privacy issues? If so, which one(s) are you most concerned with? Please select as many of the following as applicable.
   - ☐ Hacking technologies/invasion of privacy/identity theft (unprotected databases, hacking into company/government information, transaction information, information not being protected by companies/government)
   - ☐ Internet/computer use (general mention; includes mentions of 'electronic' and "wireless technologies")
   - ☐ On line social networking sites/music, video, chat (Facebook, You Tube, chat rooms, gaming sites)
   - ☐ Banking/on line banking
   - ☐ Use of cell phone/telecommunications technology/handheld devices; Personal Digital Assistant (PDA's), Blackberries, mobile devices
   - ☐ Credit cards/debit card concerns of transaction/use (cards in general)
   - ☐ Companies/Organizations selling information/sharing information/misuse of information (includes data mining, telemarketing, soliciting; includes do not call lists being misused)
   - ☐ Surveillance/tracking/recording technologies (card/licence chip technology, satellite, GPS, cameras, phone tapping, RFID's, smart cards)
   - ☐ Others – please specify
   - ☐ I am not concerned with any technologies impacting my privacy

7. Are you aware of any of the following technologies? Please select all that apply.
    a. Radio Frequency Identification (RFID) tagging
    b. Biometrics
    c. Closed Circuit Television (CCTV)
    d. Global Positioning System (GPS)
    e. None of the above

8. Are you aware of any of the following terms? Please select all that apply.

    a. Data double
    b. Dataveillance or data surveillance
    c. Digital persona
    d. Social sorting
    e. Phenetic fix
    f. None of the above

	Not at all Concerned			**Somewhat Concerned**			**Extremely Concerned**
	1	**2**	**3**	**4**	**5**	**6**	**7**
9. To what extent are you concerned about the impact technology might have on your privacy?	○	○	○	○	○	○	○

10. Have you ever been a victim of identity theft? Identity theft is the unauthorized collection and use of your personal information; usually for criminal purposes (e.g., cashing cheques in your name, withdrawing funds from your bank account, unauthorized use of your credit card).
    ☐ Yes
    ☐ No

11. Do you provide your postal code when requested by a retail store?
    ☐ Yes
    ☐ No
    ☐ I provided a fake, old, or invalid one

12. How comfortable are you with sharing personal information such as your name, address, telephone number, email address, date of birth, or financial information for each of the following?

	Not at all Comfortable			**Neither comfortable nor uncomfortable**			**Extremely Comfortable**
	1	**2**	**3**	**4**	**5**	**6**	**7**
(a) Online transactions (such as online banking, purchasing products or services over the Internet, etc)?	○	○	○	○	○	○	○
(b) Loyalty programs, such as Air Miles, reward programs at gas stations, or credit cards which allow you to collect points?	○	○	○	○	○	○	○
(c) Social networking sites such as Facebook and Twitter?	○	○	○	○	○	○	○
(d) Telemarketers?	○	○	○	○	○	○	○
(e) Government?	○	○	○	○	○	○	○
(f) Retail stores?	○	○	○	○	○	○	○

13. Have you ever experienced a serious incident where your personal information was used inappropriately or released without your consent (such as credit card information)?

☐ Yes
☐ No

14. Do you shred or destroy documents containing personal information, such as credit card offers, insurance and loan applications, bills and credit card receipts?
    - ☐ Yes
    - ☐ No

15. Have you ever reviewed an organization's privacy policy?
    - ☐ Yes
    - ☐ No

16. Do you utilize social networking websites such as Facebook? If yes, have you employed any privacy settings?
    - ☐ Yes, I use Facebook or other social networking websites, but do not use the privacy settings
    - ☐ Yes, I use Facebook or other social networking websites, and use the privacy settings to set restrictions to my profile
    - ☐ No, I do not use Facebook or other social networking sites

17. Do you believe that your personal information (e.g., name, age, address, income, e-mail address, etc.) possesses any value to others (e.g., companies, organizations, government, etc.)?
    - ☐ Yes
    - ☐ No
    - ☐ Don't know

18. Have you have ever given a store incorrect information when they ask for a name, a phone number or a postal code; to protect your personal information, or for privacy reasons?
    - ☐ Yes
    - ☐ No

19. Have you ever asked a store why they need this information when they ask for a name, a phone number or a postal code?
    - ☐ Yes
    - ☐ No

20. Have you ever refused to give a store your personal information such as name, phone number?
    - ☐ Yes
    - ☐ No
    - ☐ I gave fake, old, invalid info

21. Why did you refuse to give your personal information or give incorrect information? Please select one of the following.

- ☐ Unnecessary/they didn't need it
- ☐ Don't trust the store
- ☐ Don't want to be contacted by telemarketers/avoid junk mail/they'll try to sell me something
- ☐ Personal/private information
- ☐ None of their business
- ☐ Concerned about identity theft/fraud/computer hackers
- ☐ Safety/security issues – unspecified
- ☐ Depends on the situation/will give it on occasion
- ☐ Because I didn't want to/wasn't interested in offer
- ☐ I didn't refuse
- ☐ Other
- ☐ None/no reason
- ☐ Don't know

22. What do you think stores, organizations, etc. do with this information? Please select as many of the following that you believe apply.

- ☐ Compile statistics/demographic information on their customers
- ☐ Sell the information/sell it to telemarketers/put you on a mailing list
- ☐ Create mailing/phone lists
- ☐ Marketing/targeted marketing/increase sales
- ☐ Advertising
- ☐ Worries about confidentiality/safety/hacking and fraud
- ☐ To check my identity/credit/fraud protection
- ☐ Conduct market research
- ☐ For contact purposes/keeping track of my points/warranty/discounts
- ☐ Other – please specify
- ☐ Don't know/Refused

23. Please rate the degree to which you agree or disagree with the following statement using a 7 point scale where 1 means you strongly disagree, 7 means you strongly agree and the mid-point 4 means you neither agree nor disagree.

	Strongly Disagree			**Neither Agree nor Disagree**			**Strongly Agree**
	1	**2**	**3**	**4**	**5**	**6**	**7**
(a) I think the claims about the negative consequences of technology on the protection of personal information are overblown.	○	○	○	○	○	○	○

	1	2	3	4	5	6	7
24. I am concerned about the privacy and protection of my personal information?	○	○	○	○	○	○	○

25. Do you feel that you possess an adequate level of control over your personal information i.e., who can see and manage it; how it is distributed, and to whom it is distributed?

☐ Yes
☐ No

26. (a) Do you believe it is possible to maintain a degree of control over your personal information?

☐ Yes
☐ No

(b) If yes, do you believe that you currently have a degree of control over your personal information?

☐ Yes
☐ No

27. Have you considered the consequences of sharing personal information with others (friends, institutions, government, businesses, etc.)?

☐ Yes
☐ No

28. Please rank the following types of information in the order in which you consider them to be most personal from 1-12 (1 is most personal, 12 is least personal), and are reluctant to share?

☐ Name
☐ Age
☐ Home address
☐ E-mail address
☐ Employment status
☐ Income
☐ Marital status
☐ Health history
☐ Criminal history
☐ Credit history
☐ Educational history
☐ Driving record

	Not at all Concerned			Somewhat Concerned			Extremely Concerned
	1	**2**	**3**	**4**	**5**	**6**	**7**
29. Are you concerned about the level of accuracy, or misinformation contained in your personal file, which is held by various institutions (e.g., Ministry of Transportation, Credit Bureau, government agencies, Ministry of Education, etc.)?	○	○	○	○	○	○	○
30. Are you concerned about who views, or has access to your personal information?	○	○	○	○	○	○	○
31. Are you concerned that your personal information, held by various institutions, may be used to execute decisions about you (which may affect your chances of being granted or denied a service)?	○	○	○	○	○	○	○
32. Are you concerned that a decision about your character or personality (e.g., trustworthiness and loyalty) may be executed, solely based on particular personal information? For instance, if you are in debt, an employer may decline to hire	○	○	○	○	○	○	○

you based on the fact that because of your debt situation you are more likely to be influenced by a bribe).

33. Has your perception or view of privacy changed after having viewed the video?
    - ☐ Yes
    - ☐ No

	Not at all Concerned			**Somewhat Concerned**			**Extremely Concerned**
	1	**2**	**3**	**4**	**5**	**6**	**7**
34. Are you concerned that your personal information is collected and retained by different agencies or institutions?	○	○	○	○	○	○	○

35. Are you concerned that some of your information, contained in a database (e.g., Facebook, retail or government databases, etc.), may fall into the wrong hands (e.g., corruption; manipulation or leak of information, etc.)? Why?

_____
_____
_____
_____
_____
_____

36. How do you feel, now that you are aware of the implications involved with regards to privacy and personal information?

_____
_____
_____
_____
_____
_____

37. Does it concern you that all the personal information you have voluntarily disseminated will never be retrievable? In other words, your information is not only on paper records, but due to technological advancements, there are permanent electronic records about you everywhere. Please explain why.

_____
_____
_____
_____
_____
_____

38. Do you think the information contained about you in a database will affect you in the future? If so, how?

_____
_____
_____
_____
_____
_____

39. How do you feel about institutions using your personal information contained in a database, to make inferences and decisions about you (e.g., grant you a loan, employ you, classify you in a particular group or category, etc.)?

_____
_____
_____
_____
_____
_____

40. Will you employ particular measures to protect your personal information?

☐ Yes
☐ No

41. Are you concerned about the possibility of any misinformation (i.e., inaccurate/incorrect information) that may be contained in various databases or systems, held by other institutions?

☐ Yes
☐ No

42. Do you agree with the statement: "you have the right to privacy, but not the right to anonymity?"

☐ Yes
☐ No

43. Do you believe that Facebook uses technology, to encourage or trick its users to disclose more personal information about themselves, than they might otherwise choose to disclose?

☐ Yes
☐ No
☐ Don't know

44. Radio Frequency Identification (RFID) chips may be imbedded in some products you purchase. They emit radio waves, and can track where you take and store the item you have purchased. As a result, more information can be inferred about you.

Not at all Concerned			**Somewhat Concerned**			**Extremely Concerned**
1	**2**	**3**	**4**	**5**	**6**	**7**
○	○	○	○	○	○	○

These final questions are used for statistical purposes only.

1. Gender:
   - ☐ Male
   - ☐ Female

2. What is your year of study?
   - ☐ Undergraduate Student – First year university
   - ☐ Undergraduate Student – Second year university
   - ☐ Undergraduate Student – Third year university
   - ☐ Undergraduate Student – Fourth year university
   - ☐ Graduate Student – Masters
   - ☐ Graduate Student – PhD

3. Please indicate your discipline or program of study (e.g., Criminology, Philosophy, Law, etc.):

4. In what year were you born? Please indicate the full year; i.e., 1977 as "1977".

5. Please select your age category?
   - ☐ 18 – 19 years
   - ☐ 20 – 21 years
   - ☐ 22 – 23 years
   - ☐ 24 – 25 years
   - ☐ 26 – 27 years
   - ☐ 28 – 29 years
   - ☐ 30 years
   - ☐ Above 30
   - ☐ Above 40

6. Please select your ethnic origin:
   - ☐ **Aboriginal** (e.g., Inuit, Métis, North American Indian)
   - ☐ **African** (e.g., Black, Ethiopian, Nigerian, Somali, Sudanese, etc.)
   - ☐ **Arab** (e.g., Algerian, Egyptian, Iraqi, Jordanian, Kuwaiti, Lebanese, Libyan, Moroccan, Tunisian, Palestinian, Saudi Arabian, Syrian, Yemeni, etc.)
   - ☐ **British Isles** (e.g., English, Irish, Scottish, etc.)
   - ☐ **Caribbean** (e.g., Antiguan, Cuban, Haitian, Jamaican, Puerto Rican, St. Lucian, Trinidadian/Tobagonian, etc.)
   - ☐ **European** (e.g., Albanian, Belgian, Bosnian, Croatian, Czech, German, Greek, Italian, Latvian, Polish, Romanian, Russian, Serbian, Spanish, Swedish, Swiss, etc.)
   - ☐ **French** (e.g., Acadian, French)
   - ☐ **Latin American** (e.g., Argentinian, Bolivian, Brazilian, Chilean, Columbian, Costa Rican, Hispanic, Mexican, Nicaraguan, etc.)
   - ☐ **South Asian** (e.g., Bangladeshi, East Indian, Pakistani, Punjabi, Sri Lankan, etc.

☐ **Southeast Asian** (e.g., Cambodian, Chinese, Filipino, Indonesian, Japanese, Korean, Malaysian, Vietnamese, etc.)
☐ **West Asian** (e.g., Afghan, Armenian, Assyrian, Iranian, Israeli, Kurd, etc.)
☐ **Other** – Specify

Appendix C: Consent Form

Carleton UNIVERSITY
Canada's Capital University

Consent Form for Participants

Title of research project: Your Data Shadow

Date of ethics clearance: 6 February 2013

Ethics Clearance for the Collection of Data Expires: 31 May 2013

I, _____ volunteer to participate in a study on surveillance technologies and perception of privacy.

The purpose of this project is to determine whether creating awareness of privacy, in light of various surveillance technologies, results in a change in people's perception of privacy.

In this study, I will either ask participants to complete a questionnaire, or view a video and complete a questionnaire.

The duration of the study will vary, depending on whether the participant will view the video. The duration will therefore be between 30 minutes and one hour. The study will take place at a location convenient to the participant.

Your participation in this study is entirely voluntary. If at some point in the study you feel uncomfortable, you have the right to withdraw and cease further participation.

This study is not associated with any potential for harm. If you feel anxious during the study, please notify the researcher immediately. You may decline to answer questions that you do not feel comfortable answering and you may decide to withdraw from the study at any time. You may also withdraw your data from the study before completing the questionnaire. As the study and survey responses will be anonymous, after completing and submitting your questionnaire, there will be no way to determine or identify whose questionnaire belongs to whom. Therefore, if you choose to withdraw your data from the study, please notify the researcher before submitting your questionnaire. Participants who withdraw from the study will have their data destroyed.

Participants' responses will remain confidential, and anonymous. All surveys submitted by the participant will remain anonymous – any data you provide cannot be linked to you. The data collected during this study will be kept private and confidential. Any information that you provide will only be used by the researchers (Professor George Rigakos and Natalie Farid), for the sake of this study.

Participants will benefits from this research, as they will be educated on matters of privacy, surveillance technology and its implications, and measures which can be taken to protect themselves from fraud and identity theft.

Participants will be compensated with candy/chocolate, or pencils/pens, for their participation in this study.

The questionnaires and data collected will be stored on a USB key, which will be stored in a locked filing cabinet. The data may also be stored for future related research purposes, and will remain on the USB/data key, in a locked cabinet. Hardcopy files/questionnaires will also be filed and secured in a locked cabinet. A shredding machine will be used to destroy the data, once it is no longer needed.

The research findings of this study will be available to participants through Carleton University's Library, as well as through contact with the researcher.

Researcher Contact Information:
Natalie Farid
Carleton University Department of Law and Legal Studies
E-mail: natalie.farid@cmail.carleton.ca

This project was reviewed and received ethics clearance by the Carleton University Research Ethics Board (REB).

REB Contact Information:
Professor Antonio Gualtieri, Chair
Research Ethics Board
Carleton University Research Office
Carleton University
1125 Colonel By Drive
Ottawa, Ontario K1S 5B6
Tel: 613-520-2517, e-mail: ethics@carleton.ca

I have read the above consent form and description of the study. I understand that the data collected will be used for research as well as publishing and teaching purposes. My authorization indicates that I agree to participate in the study, and this in no way constitutes a waiver of my rights.

_____ _____
Signature of participant Date

_____ _____
Signature of researcher Date

APPENDIX D: Video Components

Title	Source	Video Link	Duration (minutes)
How is Big Brother Watching You?	CNBC	http://www.youtube.com/watch?v=MDSCC5iR_DE&feature=related	2:33
Big Brother Literally Watching and Talking to You!	British News	http://www.youtube.com/watch?v=Ze5eDmGX-lc&feature=related	1:06
Biometric - iris recognition & CCTV	UK	http://www.youtube.com/watch?v=Grg7QJGlgLc	4:19
No Place to Hide – Part 1	abc news	http://www.youtube.com/watch?src_vid=x3uBffSTWvg&annotation_id=annotation_554952&v=fIOc2YpxhxI&feature=iv	7:46
ISS Facial Recognition Security Software Highlighted on Fox News	FOX News – abp Tech	http://www.youtube.com/watch?v=94aVwIKj64M&NR=1	3:28
Facebook Adds Facial Recognition: Technology scans images, suggests names	CNN	http://www.youtube.com/watch?v=VNY3GUrjtFQ	1:41
How RFID Works	CBN	http://www.youtube.com/watch?v=yNPDgudPmXE&feature=related	2:32
Who Knows Your Secrets?	CNBC	http://www.youtube.com/watch?v=VrlO8WtZ-1Y&feature=relmfu	2:15
RFID is Pretty Cool Technology, But is it Safe and Secure?	--	http://www.youtube.com/watch?v=4avUSztf1Js	10:35
Nightline from ABC News: New Facebook Feature: Cool or Creepy?	--	http://www.youtube.com/watch?v=VQFhgk_rn6o	4:56

APPENDIX E: Statistical Tables

Table 1 *Means, Standard Deviations, and t-test*

		Control	Experimental	t-value	df
Concern about impact of technology on privacy (Q9)	M SD	5.00 1.25	5.83 0.99	-2.85**	58
Level of comfort sharing personal information in online transactions (Q12a)	M SD	4.28 1.53	3.83 1.66	1.06	57
Level of comfort sharing personal information for loyalty program (Q12b)	M SD	4.13 1.43	3.97 1.40	0.46	58
Level of comfort sharing personal information on social networking site (Q12c)	M SD	2.86 1.68	3.03 1.52	-0.41	57
Level of comfort sharing personal information with telemarketers (Q12d)	M SD	1.54 0.96	1.87 1.43	-1.03	56
Level of comfort sharing personal information with government (Q12e)	M SD	5.07 1.72	3.83 2.05	2.52*	58
Level of comfort sharing personal information with retail stores (Q12f)	M SD	3.63 1.19	3.23 1.55	1.12	58
Concern about accuracy or misinformation of personal file held by institutions (Q29)	M SD	4.10 1.75	4.73 1.68	-1.43	58
Concern about who views or accesses your personal information (Q30)	M SD	5.37 1.45	5.80 1.22	-1.26	58
Concern of personal information held by institutions and decisions made about you e.g., denial of service (Q31)	M SD	5.13 1.50	5.93 0.98	-2.44*	58
Concern about decisions regarding your character/personality made	M SD	4.83 1.91	5.97 1.03	-2.86**	58

based on particular personal information (Q32)					
Concern about personal information collected/retained by agencies (Q34)	M SD	4.97 1.33	5.73 1.11	-2.43*	58
Level of concern about RFID chips (Q44)	M SD	5.27 1.95	6.24 0.95	-2.43*	57

* $p < 0.05$.

** $p < 0.01$.

Virtually all the participants replied to these questions, with the exception of questions 12 a, c, d and 44; where no less than 28 participants replied.

Table 2

Respondents answering affirmatively to the following, to what they think of when they hear the term privacy

Question #1		Control (N = 30)	Experimental (N = 30)	X^2 (1,60)
		Count %	Count %	
Confidentiality of personal information (Q1a)		90.0	86.7	0.162
Secrecy/others not knowing your personal information (Q1b)		80.0	76.7	0.098
Security/ protection/encryption/ passwords (Q1c)		70.0	80.0	0.800
Home/family/bedroom (Q1d)		46.7	70.0	3.360
Being left alone/no solicitation/seclusion (Q1e)		46.7	56.7	0.601
Invasion/lack of privacy (Q1f)		40.0	43.3	0.069
Confidentiality of personal information (companies) (Q1g)		63.3	76.7	1.270
Confidentiality of personal information (Internet) (Q1h)		86.7	76.7	1.002
Being tracked by government (Q1i)		40.0	46.7	0.271
Freedom/non-interference/anonymity (Q1j)		36.7	63.3	4.267

* $p < 0.05$.

Table 3 (a) *Respondents' personal history with privacy*

		Control	Experimental	Control	Experimental	X^2 (1,60)
		Count %	Count %	Count %	Count %	
		Yes		**No**		
Measures/ precautions taken to protect personal information (Q2)		90.0	83.3	10.0	16.7	0.577
Victim of identity theft (Q10)		16.7	13.3	83.3	86.7	0.131
Experienced serious incident where personal information was used inappropriately/ released without consent (Q13)		13.8	13.3	86.2	86.7	0.003
Shredded/ destroyed documents containing personal information (Q14)		76.7	53.3	23.3	46.7	3.590
Reviewed an organization's privacy policy (Q15)		63.3	50.0	36.7	50.0	1.086
Given a store incorrect information, to protect personal information for privacy reasons (Q18)		46.7	46.7	53.3	53.3	0.000

Asked a store why they need personal information (19)		66.7	70.0	33.3	30.0	0.077

* $p < 0.05$.

†Question #13, only 29 out of 30 subjects from Group 1 responded to the question.

Table 3 (b) *Perceptions of control about privacy*

	Control	Experimental	Control	Experimental	X^2 (1,60)
	Count %	Count %	Count %	Count %	
	Yes		**No**		
Possess an adequate level of control over personal information (Q25)	66.7	33.3	33.3	66.7	6.667*
Possible to maintain control over personal information (Q26a)	83.3	50.0	16.7	50.0	7.500*
Currently have control over personal information (Q26b)	66.7	36.7	16.7	13.3	7.724*
Considered consequences of sharing personal information with others (Q27)	86.7	86.7	13.3	13.3	0.000
Will you employ measures to protect personal information (Q40)	90.0	96.7	10.0	3.3	1.071
Concerned about possibility of misinformation contained in various databases of institutions (Q41)	72.4	83.3	27.6	16.7	1.023
Agree with: right to privacy but not anonymity (Q42)	30.0	13.8	70.0	86.2	2.255

* $p < 0.05$.
** $p < 0.01$.
†Question #41, only 29 out of 30 subjects from Group 1 (Control) responded to the question.
†Question #42, 29 out of 30 subjects from Group 2 (Experimental) responded to the question.

Table 4

History of respondents' experience with matters of privacy

	Control			Experimental			X^2 (1,60)
	Count % Yes	Count % No	Count % Other	Count % Yes	Count % No	Count % Other	
Providing postal code to retail store when requested (Q11)	76.7	20.0	3.3	63.3	20.0	16.7	3.048
Belief that personal information possesses value to others (Q17)	83.3	6.7	10.0	66.7	3.3	30.0	3.889
Refused to give store your personal information (Q20)	46.7	33.3	20.0	50.0	46.7	3.3	4.273
Belief that Facebook uses technology to encourage/trick users to disclose more of their personal information (Q43)	70.0	16.7	13.3	79.3	0.0	20.7	5.476

* $p < 0.05$.

†Note: Question # 43 – total number of subjects from Group 2 who responded to the question was 29, not 30 (therefore, 1 less).

†The category “Other” for question #11, the option on the Questionnaire is “I provided fake, old, or invalid one”; and for question # 20, the option is “I gave fake, old, invalid info”.

†The category “Other” for questions #17 and 43, the option on the Questionnaire is “Don’t know”.

Table 5

Question 33: Has your perception or view of privacy changed after having viewed the video?

		N	Group 2		X^2 (1,28)
		28	Count % Yes	Count % No	4.929*
Male		8	62.5	37.5	
Female		20	95.0	5.0	

* $p < 0.05$.

Table 6

Question #7		Control	Experimental	Control	Experimental	X^2 (1,60)
		Count %	Count %	Count %	Count %	
		Not Selected		**Selected**		
(a) Radio Frequency Ident-ification (RFID) tagging		70.0	30.0	30.0	70.0	9.600**
(b) Biometrics		76.7	16.7	23.3	83.3	21.696**
(c) Closed Circuit Television (CCTV)		46.7	26.7	53.3	73.3	2.584
(d) Global Positioning System (GPS)		16.7	6.7	83.3	93.3	1.456
(e) None of the above		83.3	100.0	16.7	0.0	5.455

* $p < 0.05$.
** $p < 0.01$.

Table 7

Question #8		Control	Experimental	Control	Experimental	X^2 (1,60)
		Count %	Count %	Count %	Count %	
		Not Selected		**Selected**		
(a) Data Double		96.7	53.3	3.3	46.7	15.022**
(b) Data-veillance or data surveillance		36.7	23.3	63.3	76.7	1.270
(c) Digital persona		53.3	63.3	46.7	36.7	0.617
(d) Social sorting		76.7	66.7	23.3	33.3	0.739
(e) Phenetic fix		100.0	90.0	0.0	10.0	3.158
(f) None of the above		70.0	83.3	30.0	16.7	1.491

* $p < 0.05$.
** $p < 0.01$.

Table 8

Question 4:

			Control	Experimental	t-value	df
I have enough information to know how new technologies might affect my personal privacy. (Q4a)		M SD	4.50 1.503	3.93 1.721	1.359	58
I take adequate precautions to protect my information on social networking sites such as Facebook. (Q4b)		M SD	4.90 1.520	4.37 1.810	1.216	57
Even if my privacy is breached, the consequences are not significant. (Q4c)		M SD	3.33 1.988	2.10 1.348	2.812**	58
I am concerned about personal information becoming public that may be embarrassing to me. (Q4d)		M SD	4.87 1.795	5.23 1.654	-0.823	58
I am concerned about the financial risk of online commerce. (Q4e)		M SD	4.80 1.690	5.31 1.775	-1.131	57
I am concerned that my friends might end up providing information to others about me through social networking. (Q4f)		M SD	3.87 1.717	5.20 1.495	-3.208**	58
I am concerned that corporations might end up using information about me that I didn't approve of or know about. (Q4g)		M SD	5.10 1.807	6.23 1.006	-3.001**	58
I am concerned that the government might end up using information about me that I didn't approve of or know about. (Q4h)		M SD	4.60 1.940	6.27 1.048	-4.139**	58

* $p < 0.05$.
** $p < 0.01$.

Virtually all the participants replied to this question, with the exception of 4b (control group) and 4e (experimental group); where no less than 29 participants replied.

Table 9

			Control	Experimental	t-value	df
In your day to day life, how good of a job would you say you are doing to protect the privacy of your own personal information? (Q3)		M SD	3.40 0.724	3.10 0.923	1.401	58
How important is it to you personally to have strong laws to protect Canadians' personal information? (Q5)		M SD	6.03 1.351	6.00 1.114	0.104	58

* $p < 0.05$. All the participants replied to these two questions.
** $p < 0.01$.

Table 10

Consequences and concerns regarding protection of personal information

			Control	Experimental	t-value	df
I think the claims about the negative consequences of technology on the protection of personal information are overblown. (Q23)		M SD	2.87 1.502	2.30 1.418	1.502	58
I am concerned about the privacy and protection of my personal information. (Q24)		M SD	5.67 1.061	6.07 0.980	-1.516	58

* $p < 0.05$. All the participants replied to these two questions.
** $p < 0.01$.

Table 11

Respondents' answers regarding use of Facebook (social networking website)

Question 16: Do you utilize social networking websites such as Facebook? If yes, have you employed any privacy settings?

Question #16		Control (N = 30)	Experimental (N = 30)	X^2 (2,60)
		Count %	Count %	
Yes, I use Facebook or other social networking websites, but do not use the privacy settings		10.0	10.0	
Yes, I use Facebook or other social networking websites, and use the privacy settings to set restrictions to my profile		76.7	80.0	.164
No, I do not use Facebook or other social networking sites		13.3	10.0	

* $p < 0.05$. All participants replied to this question.

Table 12 *Privacy concern regarding new technologies*

Question #6	Control (N = 30)	Experimental (N = 30)	Control (N = 30)	Experimental (N = 30)	X^2 (1,60)
	Count %	Count %	Count %	Count %	
	Not Selected		**Selected**		
(a) Hacking technologies/ invasion of privacy/identity theft (unprotected databases…)	10.0	10.0	90.0	90.0	0.000
(b) Internet/ computer use	63.6	46.7	36.7	53.3	1.684
(c) On line social networking sites/ music, video, chat (Facebook etc.)	40.0	26.7	60.0	73.3	1.200
(d) Banking/on line banking	33.3	30.0	66.7	70.0	0.077
(e) Use of cell phone/ telecommunications technology/ handheld devices; Personal Digital Assistant, Blackberries, mobile devices	70.0	40.0	30.0	60.0	5.455*
(f) Credit cards/debit card concerns of transaction/use	23.3	16.7	76.7	83.3	0.417
(g) Companies/ Organizations selling information/ sharing information/ misuse of information (data mining…)	46.7	23.3	53.3	76.7	3.590

(h) Surveillance tracking/recording technologies (chip technology, GPS, RFID etc.)	50.0	20.0	50.0	80.0	5.934*
(i) Other – please specify	100.0	90.0	0.0	10.0	3.158
(j) I am not concerned with any technologies impacting my privacy	Not Applicable				

* $p < 0.05$.

Table 13

Thoughts regarding what stores and organizations do with personal information

Question #22	Control (N = 30)	Experimental (N = 30)	Control (N = 30)	Experimental (N = 30)	X^2 (1,60)
	Count %	Count %	Count %	Count %	
	Not Selected		**Selected**		
(a) Compile statistics/ demographic information on their customers	13.3	20.0	86.7	80.0	0.480
(b) Sell the information/sell it to telemarketers/put you on a mailing list	53.3	40.0	46.7	60.0	1.071
(c) Create mailing/ phone lists	16.7	20.0	83.3	80.0	0.111
(d) Marketing/ targeted marketing/ increase sales	26.7	20.0	73.3	80.0	0.373
(e) Advertising	26.7	40.0	73.3	60.0	1.200
(f) Worries about confidentiality/ safety/hacking and fraud	96.7	80.0	3.3	20.0	4.043
(g) To check my identity/credit/fraud protection	93.3	66.7	6.7	33.3	6.667*
(h) Conduct market research	36.7	33.3	63.3	66.7	0.073
(i) For contact purposes/keeping track of my points/ warranty/discounts	48.3	46.7	51.7	53.3	0.015
(j) Other – specify	93.3	96.7	6.7	3.3	0.351

(k) Don't know/Refused	Not Applicable

* $p < 0.05$.

†Note: Question # 22 (i) One participant from the control group did not reply to this question (i.e., 29 out of 30 responded).