The Data Fishbowl

An Ethical and Philosophical Analysis of Information Privacy in an Integrated Digital World

Master's Thesis – Public Ethics

John W. Ekholm

Thesis Advisor: Prof. Gregory J. Walters (Ph.D.)

December 2013

Saint Paul University, Ottawa

The Data Fishbowl

An Ethical and Philosophical Analysis of Information Privacy in an Integrated Digital World

Abstract

Advancements in technology and the advent of the global digital information infrastructure, while offering great benefits, have concurrently eroded privacy and have left us vulnerable to a broad range of ills. "Privacy invasion creep" has progressed to the extent that it raises questions about the future of privacy, its continued viability, and even its relevance. It also raises questions about the value, and perhaps futility, of our attempting to preserve it.

This thesis examines privacy, particularly *information* privacy, in today's high-tech environment from various philosophical and ethical perspectives with the aim of shedding light on these issues and, ultimately, to help guide future institutional discussions and decisions on privacy-related matters. To this end, I set out to prove that 1) privacy remains highly relevant on both individual and societal levels, and 2) its restoration and preservation constitutes an ethical imperative. I begin by highlighting the more significant developments that have impacted privacy, to provide context. I then argue in support of privacy's continued relevance from three perspectives—psychological, sociological and fundamental rights. I also identify risks inherent in its encroachment and point to societal responses that these risks and impacts have prompted in various jurisdictions. Finally, I offer four ethical perspectives—based on the philosophical doctrine of John Stuart Mill, Immanuel Kant, John Rawls and Alan Gewirth—on the moral requirement to restore and preserve privacy.

Upholding the first assertion, the evidence presented indicates that privacy is indispensable for emotional well-being and for the social fabric of society, and that it deserves consideration as a human right. It also demonstrates the importance that is widely attributed to privacy, as well as its viability, partly through the many initiatives undertaken to support it. The arguments that are subsequently presented based on each of the four ethical perspectives bear out the second assertion, that the preservation and restoration of privacy constitutes an ethical imperative. I conclude with the finding that the erosion of privacy to date and the current trends give cause for serious concern, sober reflection, and collective action.

Table of Contents

Page

1. Introduction

1.1 The Problem

More than ever, we communicate and conduct business through the global digital information infrastructure (GII). We even publicly post personal information, both pictorial and verbal, and in many instances we do this despite known inherent vulnerabilities and risks to privacy. Previously unimaginable amounts of personal information, and information in general, are now readily available to persons and institutions—private and public alike—regardless of geographic location. Data on purchases made online or with the use of debit and credit cards let us fall prey to ad campaigns, spam, spyware, the selling of personal information about us to marketers and others, and worse.

Many of us, certainly in the industrialized world, are routinely subjected to audio and video recording, access card and body scanning, biometric and genetic information gathering and processing, and tracking of cell phone use and location, as well as debit and credit card expenditures and, of course, locations of use. Photos of our homes are taken without our knowledge or consent and made available to the world.

The GII in general and the Internet in particular—which alone has made possible, and seen, an increase in the movement and retention of data worldwide by several orders of magnitude since its inception—lend themselves exceptionally well to surveilling and exploiting people, including monitoring their activities, accessing and distributing personal information, targeting them for advertising, and invading privacy in general. In part, this is because that environment is so information rich and is used so extensively by virtually everyone in the civilized world; but it is also because the cyber world does not pose the same

challenges for such activities as does the concrete, bricks-and-mortar world, where surveillance, stalking and other forms of information gathering and exploitation are much more difficult to conceal. Online, countless Internet service providers (ISPs), social media organizations and other corporate entities engage in such activities continually and on a large, even massive, scale, building profiles of our habits and preferences—everything we type, every link or picture we access, every page we read, every bit of information we download. And this information may be stored indefinitely. Some of it is even sold.

It is not only industrial and commercial entities that are monitoring personal online activity and collecting, using and distributing personal information more than ever; governments are doing it as well. Why? Because the GII, which includes the Internet, has become the primary means for communication overall, including moving and processing information required for governments to operate and to provide convenient and timely services to the public. Such monitoring and information sharing also helps with crime prevention and prosecution, including, but certainly not limited to, cybercrime[1] and cyber-terrorism,[2] the latter of which stems from the increasing functional dependence of many of our critical infrastructures on globally accessible information networks.

Consequently, the state of privacy is not what it was in the pre-Internet era, before the explosion of the digital economy and the emergence of globalized surveillance; rather, privacy has lost significant ground. In fact, "privacy invasion creep"—or what Judith DeCew (2013) refers to as the "clash between privacy and technology"—has progressed to such an extent and gathered such momentum that, despite various elaborations of privacy legislation

[1] Cybercrime is defined herein as crime committed remotely both via and in relation to information networks or systems, including computers, normally through the Internet or global information infrastructure.
[2] Cyber-terrorism is defined herein as acts of terrorism committed via information networks or systems.

and considerable efforts of privacy advocates, it raises questions about the continued viability, and even relevance, of privacy—especially information privacy—as a concept, as a social value and, to the extent it has been recognized as such, as a human right.

1.2 Current State of Affairs

Advancements in technology and the advent of the global digital information infrastructure, while unquestionably offering vast new opportunities, conveniences and other benefits, including new means to *enhance* privacy, have concurrently and unequivocally eroded our ability to safeguard at least certain aspects of privacy. While information and other technologies have continued to advance, industrialized societies have, for the most part, watched privacy gradually diminish and can claim only limited accomplishments by way of taking advantage of the same technological progress to actually *enhance* privacy, or even to help offset its decline. Admittedly, much of our conduct—including our ever-increasing use of and reliance upon new information technologies and associated infrastructures, in general, and many of our social media behaviours, in particular—could be, and indeed often are, interpreted to suggest that our privacy is of little concern or interest to us. But others have found that privacy remains of utmost importance to most people, albeit perhaps with somewhat different expectations compared to a generation or more ago. Some have offered at least a partial explanation by submitting that, in our integrated digital world, privacy has become perceived as futile, and its very concept, therefore, moot, especially when the use of electronic media, along with the associated vulnerabilities and risks, has become the norm—even sine qua non—for conducting many types of business. Moreover, in a highly developed and regarded country like Canada we have a general tendency to trust in the inherent

robustness and security of our critical infrastructures, given the accepted expertise of our service providers and assumed wisdom, integrity and omnipotence of the government institutions charged with regulating and overseeing these infrastructures. This propensity certainly applies in relation to *information* infrastructures, including the protection of privacy and the presumed safe handling of personal information, likely due , in part, to the formal establishment—and, in recent years, elaboration—of institutions, policies and even legislation specifically concerned with such matters.

In terms of the literature that has been published on this subject, a seemingly almost endless supply of information has been disseminated about privacy threats arising from globalization, technological evolution and such, whether by the media, privacy commissioners and advocacy groups, technology journals and publications, assorted futurists, or other authors. Somewhat less, but still a considerable amount, has been written about the social and psychological implications of this development (Allen, 1988; Bloustein, 1964; Chandler, 2009; Davies, 1997; Fried, 1970; Inness, 1992; Johnson, 2009; McFarland, 2012; Moore, 2000, 2003, 2010; Rachels, 1975; Shade, 2008; Solove, 2008; Steeves, 2009; Uteck, 2009; Walters, 2001; Westin, 1967; etc.). Relatively little has been written, however, that offers philosophical and ethical perspectives on the issue of privacy, in particular *information* privacy, within the context of advancing communications and information technology and our increasingly interconnected and integrated digital world (e.g., Guyer (1998), Johnson (2009) and McFarland (2012) have offered Kantian insights of relevance to the issue; Walters (2001) has addressed the issue of privacy in considerable depth from a Gewirthian perspective, albeit not aimed specifically at information privacy within said context). A treatment of the subject

that offers multiple ethical perspectives, as in the case of the present thesis, constitutes virtually uncharted territory.

1.3 Objective

The foregoing raises questions such as the following: In what ways and to what extent has the advent of the global digital information infrastructure impacted privacy? Is privacy on a path toward becoming futile and obsolete? Why does it matter? It is with the aim of shedding light on these issues that this thesis examines the state of affairs regarding privacy, in general, and *information* privacy, in particular, within the context of our technological environment. More specifically, it considers the impact that the arrival of the information era has had on modern society's privacy interests and expectations, and explores the relevance of the concept of privacy in today's high-tech environment from psychological, social, philosophical and ethical perspectives.

The ultimate objective of this exploration is to enlighten and help focus and direct future institutional discussions and decisions on privacy-related matters, to the benefit of all modern societies.

1.4 Hypothesis

Despite the pervasiveness of "privacy invasion creep" owing to the evolution and exploitation of technology, privacy as a concept remains highly relevant at both the individual and societal levels, based on three broad perspectives—psychological, sociological and fundamental rights—and its preservation and restoration constitutes an ethical imperative.

1.5 Methodology

I begin by highlighting some of the more significant developments—particularly in relation to communications and information technology—that have most profoundly impacted privacy. While this subject area has been extensively covered in assorted literature, it nevertheless merits review, consolidation and summarization herein given its contextual significance to my hypothesis. I then argue in support of the continued relevance of privacy from three perspectives—psychological, sociological and fundamental rights. I also identify risks inherent in its encroachment and later present some of the societal responses that these privacy risks and impacts have prompted in various jurisdictions. The purpose of this is twofold: first, it serves as a testament to the importance that societies continue to attribute to privacy, and, second, it indicates the outstanding call, and need, to maintain and protect privacy in the face of today's challenges and threats to privacy, as well as to seek out, recognize and seize the opportunities for rehabilitating and *enhancing* privacy that the information age and the continual generation of new technologies and applications certainly offer. Finally, I present four ethical perspectives—based on the philosophical doctrine of John Stuart Mill (utilitarian), Immanuel Kant (monistic deontological), John Rawls (social contract theory with deontological underpinnings) and Alan Gewirth (ethical rationalism)—on the moral requirement to restore and preserve privacy.

2. What Happened to Privacy, and Why?

2.1 Privacy Defined

When discussing a concept as broad as privacy it is often useful, if not essential, to define its scope for the purposes of that discussion at the outset. Such delineation would seem particularly appropriate in regard to privacy because its widely varying historical use and interpretations have rendered it a comparatively nebulous term. To cite a few examples, Aristotle viewed privacy within the context of activities and information pertaining to the familial sphere or domain (the *oikos*), as compared to the political domain (the *polis*). John Stuart Mill (1869), in his essay *On Liberty*, differentiates between the public and private domains by placing the former within the realm of government authority and the latter within the realm of self-regulation. John Locke (1690), in his *Second Treatise on Government*, speaks of privacy in terms of one's body and oneself as well as private property, which, according to him, one acquires by combining one's labour with the world's—i.e., public—bounty (Locke, cited in DeCew, 2013). Privacy can refer to, among other things, "a sphere separate from government, a domain inappropriate for governmental interference, forbidden views and knowledge, solitude, or restricted access" (DeCew, 2013). Daniel Solove opines that privacy is currently "a concept in disarray," a broad concept that includes, inter alia, "freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations" (2008, p. 1).

The focus of this thesis is *information* privacy, which I am defining as the ability to control, or at least significantly influence, the collection, retention, use and promulgation of

personal information about oneself, as an individual, regardless of whether that information is fact-based (e.g., financial, biological, or actions-based), visual (e.g., pictorial), cerebral (e.g., thoughts, beliefs, emotions), or otherwise. It is this aspect of privacy—as compared to, say, physical isolation or protection from unwanted physical intrusions—that has been most notably impacted by the advent of the information era and the creation of the global digital information infrastructure. Moreover, while it can be argued that corporate, business or organizational privacy has also been significantly impacted, the scope of that impact is much narrower, given the relative absence of many of the facets of information privacy that are of a personal nature.

Although the focus of the thesis is information privacy, the subject cannot be adequately addressed in complete isolation from a broader conception of privacy and the contextual enlightenment that a more inclusive treatment offers. Hence, at times I deliberately speak of privacy in a very broad sense so as to allow a more multi-dimensional and fulsome treatment of the subject at hand. Given the dialectical nature of the discussion and the breadth and complexity of the concept of privacy writ large, I submit the following as a working definition of "privacy" for the purposes of this thesis, in the interest of clarity: the absence of unwanted intrusions on what might reasonably be considered one's personal, private, confidential or intimate self, whether those intrusions are physical (e.g., pertaining to one's body, personal space, property, activities) or informational (i.e., pertaining to personal information, as elaborated above). In cases where I am specifically referring to the narrower tranche of privacy that is *information* privacy, I have undertaken to so indicate.

I would like to offer two points of clarification before proceeding to the next section. First, William Parent (1983) defines privacy as the condition of not having private (i.e., "non-

public") personal information known or possessed by others. This suggests that the instant that personal information becomes known to anyone other than the person to whom that information pertains, it is no longer private and, therefore, that any regime that has been established or obligation imposed in relation to information privacy no longer applies. I would argue, however, that the notion of privacy can still apply in instances where "non-public" information has been shared in confidence with one or more selected individuals, such as a family member, close friend, confidant, et cetera, and where the intent was, and remains, that further dissemination would not occur unless so sanctioned by the originator. Second, when discussing privacy and its protection, one might be inclined to ask, From whom exactly are we seeking privacy—government institutions, corporations and businesses, private individuals, all of the above? I wish to clarify here that, because the focus of information privacy is on controlling information about oneself, the field of potential actors from whom privacy may be sought in any given instance is essentially without limitation.

2.2 Trends and Developments

More than ever privacy is threatened and continually impacted by technology and its advancement. As technology, in particular *information* technology, has evolved, so have the ways in which privacy is encroached upon. Going far back in time, one major development that impacted privacy was the invention of the printing press in the 15th century, which dramatically enhanced the capability to disseminate information. Stories and information previously shared with just a handful of people by word of mouth or written by hand suddenly became readily available to the multitudes. A few centuries later, in and about the 1800s, technological innovation brought the telegraph and the camera into popular use. Mass

distribution became the order of the day, and pictures and stories about individuals, once limited to a very small group of persons who were mostly known to the subject, became broadly disseminated to unknown persons in other regions of the country and even the world. Yet these developments pale in comparison to the much more recent advent of high-resolution miniaturized cameras, ultra-high-definition satellite imagery, unmanned surveillance drones, Global Positioning Satellites (GPS), high-gain microphones, integrated circuits and computer microchips, biotechnology, nanotechnology, and, of course, communications technology, the Internet and the broader global information infrastructure, all of which, though offering remarkable opportunities for quality of life improvement, have concurrently made the availability of personal information, and the ways that privacy can be infringed, immeasurably greater than ever before.

Our business phone calls are becoming routinely recorded—ostensibly for training purposes and to improve customer service—as are many of our actions routinely recorded on cameras—video cameras located on buildings, in hallways, on buses, by roadways, even in some public washrooms, to enhance security or to monitor traffic conditions. Other cameras have been installed to catch traffic violations at select intersections or to identify vehicle license plates on toll highways, to name but a couple of their applications. Photographs of our homes are taken without our prior knowledge or consent and made available to the world. In many instances employees are monitored in the workplace through video cameras and/or surveillance of their online activities.

We are subjected to body scanning at airports, at many store exits and at assorted other venues for security purposes. Biometric data is increasingly gathered via fingerprints, retinal scanning, voice recognition, digital photography and facial recognition technology. Even data

about our DNA, the complete genetic blueprint for us as unique and individual human beings, is readily obtained from a sample of blood, urine, feces, saliva, hair, or any other of our billions of body cells. There is increasing concern that, in the not-too-distant future, DNA information will be used in determining medical and life insurance rates and even to determine whether to provide insurance coverage at all.

Mobile communication service providers generate, and maintain indefinitely, detailed records of our usage of cell/smart phones and other wireless devices. Further to the obvious records of with whom we communicated, when and for how long, the actual content of our communications is also vulnerable to infringement. Adding to that vulnerability, cellular technology also allows tracking of our approximate location at any time, provided that our mobile communication device is turned on and is not in "flight" mode. That said, the precision with which our location can be determined through such devices pales in comparison to the accuracy and precision of our location when our mobile device is using a GPS-based location service. In the latter instance one's location can be determined within about one square metre, versus within a few square blocks, as in the case of cell tower usage. The upside of having precise GPS geo-location capabilities is that we can enjoy the obvious benefits of high accuracy when receiving travel directions and related services, or if we are injured and need to be precisely located to receive help; the down side, however, is that detailed records of our movements are created, held by others, and not at all within our control.

Access cards, debit cards and credit cards with magnetic stripes or computer chips, used for everyday business transactions, can store vast amounts of personal information and can be used to track our expenditures, buying habits, locations and dates/times of purchases,

and much more. A particularly recent development has been the advent of the smart public transit pass, which ostensibly improves transit efficiency, albeit at the privacy expense of having records created—again that are not within our control—of when and where we boarded a public transit vehicle.

For years there has been talk of a single universal government-issued ID card to be used for all government services, including health services, driver's license renewal, passport applications, obtaining old age security benefits, et cetera. This would enable single-card access to health records, social insurance numbers, date and place of birth, driving and criminal records, passport information, travel records, income and tax records, and more. The potential for privacy encroachment and secondary or derivative forms of information abuse is significant. In one year (November 2012 – November 2013) in Canada alone there were several reported cases of public sector organizations having compromised privacy through reckless or negligent handling of sensitive personal information. In one instance, it was discovered that a hospital employee had misplaced a USB key containing personal information for more than 25,000 of the hospital's patients, including names, "summary data relating to the type of service received, the date of service, and a code referring to the doctor's name" (Laucius, 2013, April 5, p. C2). The data had been downloaded onto the employee's personal USB key, reportedly contrary to hospital rules, was not encrypted, and became lost for several months after the employee removed it from the hospital premises with the apparent intention to carry out work at home over the weekend.

In another, well-publicized case, a USB key containing personal information on 5,045 Canadians and a hard drive with personal information on an additional 583,000 Canadians were discovered missing from two offices of Human Resources and Skills Development

Canada (HRSDC). Both devices contained personal information that was deemed to be sensitive and neither were encrypted. The information on the hard drive related to Canada Student Loan borrowers and included "names, social insurance numbers, dates of birth, addresses and loan balances—enough information for criminals to steal someone's identity" (Press, 2013, January 18). The incident resulted in several reported cases of actual identity theft and at least three class-action lawsuits over the data and related privacy breaches (Press, 2013, January 19).

In yet another case, albeit not related to information technology per se, the privacy of a Department of National Defence (DND) employee was deemed by the Privacy Commissioner of Canada, following a complaint, to have been violated when the Department released personal information to the media in relation to the employee's leave status and the personal grounds for that leave. The disclosed information revealed that the employee had been in a close, and sensitive, personal relationship with another individual of the same sex, who had just been the victim of a homicide. The DND employee was subsequently fired from his job, owing, he claimed, to his relationship with the deceased (Hurley, 2013, January 18).

More recently, there was an instance where Health Canada sent letters to some 40,000 approved, legitimate medical marijuana users to inform them of certain upcoming changes to their drug program. Regrettably, the letters arrived in an envelope on the outside of which was an explicit reference to the Medical Marijuana Access Program as well as the name of the patient. Consequently, as one program participant put it, "the gaffe has painted a target on the backs of medical marijuana patients across Canada, many of whom now fear home invasions" (Health Canada gaffe, 2013, November 22). A law firm subsequently filed a proposed class-

action lawsuit against Health Canada for allegedly violating the privacy of medical marijuana users (Medical marijuana privacy breach, 2013, November 26).

As my last example, it was reported in October 2013 that Jennifer Stoddart, then Privacy Commissioner of Canada, had blamed weak security practices at the Canada Revenue Agency for thousands of files containing sensitive personal information having been inappropriately accessed for years without detection. In a news release she maintained that "Canadians deserve to have their personal information protected, particularly when they provide it to the government under legal compulsion" (Lax security, 2013, October 29). It was also reported that, for the second year in a row, record highs had been reached for privacy complaints received by the Privacy Commissioner about federal government departments and agencies (2,273 for fiscal year 2012-2013 versus 986 for the same period a year earlier) as well as for data breaches reported by government organizations (Lax security, 2013, October 29).

Finally, there is the GII and the Internet, which deliver such communication services as conventional world-wide telephony, video-conferencing, media broadcasting and, of course, a wide assortment of World-Wide Web (hereafter "Web") services, such as net-banking, e-mailing, Web surfing, online shopping, gaming, social media (e.g., Facebook, MySpace, Twitter, YouTube), free voice telephony, using voice-over Internet protocol (VoIP), and video-telephony (e.g., "Skyping"). Most of these services are accessed through an intermediary (e.g., telecommunications carrier or ISP), which receives payment for its services. There are numerous obvious benefits offered by the advent of the Internet, in the late 1980s, and its explosive growth throughout the 1990s and in the years since. However, privacy has not been one of them. Leslie Regan Shade (2008, p.80) makes reference to "the

current challenges of emergent material technologies accelerated by digitization and political technologies of regulation and governance," recognizing that privacy has never been more challenged than it is currently, and that this is largely owing to recent advances in information and communications technology, in general, and the arrival of the Internet, in particular, whose rapid evolution has well outpaced the ability—and, in some instances, willingness—of legislators, policy makers and regulators to properly govern it.

Unprecedented amounts of data, including personal information, are collected, stored, moved, shared, and used, mostly without even the awareness, let alone consent, of the individual to whom the information pertains. Data, such as emails, are stored on business computer servers and other storage devices even if "deleted" by the user. There are mammoth databases and Internet records on individual financial and credit history, medical records, purchases, telephone calls, Web browsing history, and so forth, and most people don't know what information about them has been collected and is being stored, or who has access to it. More than ever databases are being cross-linked to facilitate information sharing, thereby further widening the circle of those who have access to the information. Moreover, there are few controls over the handling of such information, particularly across the private sector. This is partly due to the multi-jurisdictional nature of the Internet and partly due to the virtual explosion in demand for Internet services at the outset, as a consequence of which the accelerated pace and abbreviated timetables for design, development and implementation afforded little time, opportunity and, frankly, incentive for security and, especially, privacy issues to be fully considered and addressed in a robust manner. Fortunately, law enforcement and national security organizations, along with other government entities, generally operate within a defined legal framework and have policies, internal controls and external review

mechanisms in place to mitigate risk to privacy, both in relation to the Internet and otherwise; however, the same does not hold true in regard to the private sector, even when bound by privacy legislation.

Andrew Grove, co-founder and former CEO of Intel Corporation, has been quoted by numerous sources as having lamented, in 2000, "Privacy is one of the biggest problems in this new electronic age." In her 2005- 2006 *Annual Report*, Canadian Privacy Commissioner Jennifer Stoddart commented on the ability of digital technologies to jeopardize personal privacy, noting that they have created "limitless storage capacities, limitless transmission capacity, limitless data mining capacity . . . the challenge of protecting data is increasingly globalized, because actions in one distant part of the world now may directly impact the privacy of Canadians" (Stoddart, cited in Shade, 2008, p.85). Stoddart also pointed out that developments in information and communications technology "make citizens vulnerable to surveillance manipulation through personal information gathered by search engines and data mining" (Stoddart, cited in Shade, 2008, p.85). According to privacy advocate Jeffrey Chester, "This information can be collected and stored to create detailed profiles of user tastes and preferences in shopping, reading, and other habits, all of great value to corporations that rely on mass marketing" (Chester, cited in Shade, 2008, p.85). Children and youth are especially vulnerable to privacy threats posed by their Web surfing activities and the associated data mining by marketers, who are using increasingly stealthy techniques. This "raises important ethical issues about children's rights to privacy and freedom of expression" (Shade, 2008, p. 85).

In 2007, Carolyn Bassett warned that we are on a "total surveillance trajectory" (Bassett, cited in Shade, 2008, p.85). Adding to Bassett's warning, Leslie Regan Shade

contends, “Globalization, convergence, and the malleability of multimedia have created a fascinating and often conflicted landscape wherein individual privacy is becoming rapidly eroded” (Shade, 2008, p. 85).

2.3 Drivers and Incentives

It is often said that knowledge is power. It has also been said repeatedly that information (a key component of knowledge) is money. So there is abundant incentive for actors to tap into the global information network and attempt to access much of the information that resides on it. The seemingly limitless arsenal of spyware and social engineering products residing on the Web—or in “cyberspace”—serves as both a testimonial and indicator of the validity of these maxims.

In recent years there have been numerous reports about governments, including especially the U.S. federal government, cooperatively monitoring Internet activities, and even gaining access to supposedly secure encrypted data, to facilitate the identification, tracking and thwarting of potential threats to national security. This, quite justifiably, has led to a reduced general sense of privacy within our integrated digital environment, owing in part to a perceived rivalry between national security and privacy. Particularly post-9/11, people in the industrialized Western world, have become more accepting than ever of the notions that privacy is in competition with national security and that national security is a prerequisite to enjoying any benefits of privacy (or, for that matter, almost anything else that we value). In a real sense, we have implicitly entered into a social contract with the state whereby we have agreed to give up some personal rights and freedoms, including some degree of privacy, in

return for security and protection provided by a legitimate political authority. A factor contributing to this change has been the reality that privacy as a concept remains, for the most part, relatively vague and intangible, whereas the concepts of security and the associated risks of its failure are more tangible, easily visualized and readily perceived as real and highly significant—a phenomenon that psychologists refer to as the "availability heuristic" (Chandler, 2009, p. 127).

In addition, security as a value may be more compelling than privacy simply because *more* tends to be viewed as *better*, whereas privacy is generally not viewed in the same light. There is also what has been referred to as the "rally effect," where people are increasingly inclined to support and trust, at least temporarily, their political leadership following a major traumatic incident (Chandler, 2009, p. 131). The events of September 11, 2001 present a perfect case in point and may well have incited people in at-risk nations during the years that followed (and even to this day) to defer concerns over privacy in favour of helping the authorities re-establish a homeland that is perceived to be free from future such threats and to seek justice against the perpetrators of the atrocious acts. The rally effect might have been a factor in events surrounding the Maher Arar case, wherein multiple law enforcement agencies committed privacy violations under the pretext of national and global security (O'Connor Commission, cited in Shade, 2008). All of these factors, in addition to the notion that survival, and hence security, is essential to enjoying the fruits of all liberties and values, may have contributed to what can easily be perceived as recent general complacency by the public in regard to privacy and its encroachment (Chandler, 2009).

The December 2013 report of the Review Group on Intelligence and Communications Technology, which was set up by U.S. President Obama in the wake of Edward Snowden's allegations in relation to the National Security Agency, provides the following commentary on the historical tendency to favour "security" over "liberty" (including privacy) during periods of perceived crisis:

> *"... it is always challenging to strike the right balance between the often competing values of national security and individual liberty, but as history teaches, it is particularly difficult to reconcile these values in times of real or perceived national crisis. Human nature being what it is, there is inevitably a risk of overreaction when we act out of fear. At such moments, those charged with the responsibility for keeping our nation safe, supported by an anxious public, have too often gone beyond programs and policies that were in fact necessary and appropriate to protect the nation and taken steps that unnecessarily and sometimes dangerously jeopardized individual freedom. This phenomenon is evident throughout ... history. Too often, we have overreacted in periods of national crisis ... in such periods, there is a temptation to ignore the fact that risks are on all sides of the equation, and to compromise liberty at the expense of security" (cited in NSA review panel findings: Liberty and Security in a Changing World, 2013, December 18).*

While Jennifer Chandler acknowledges that there may be a legitimate need for a limited trade-off between privacy and security in certain contexts, she also warns that depicting this need as a contest between the two values tends to prematurely curtail debate in favour of security (2009). The danger posed by this scenario—i.e., where national security is prematurely permitted to trump other values that are viewed to be in competition with it—is that some key considerations, such as the following, might not receive adequate attention:

1) whether the contemplated security measure actually delivers any security;
2) whether there is a less privacy-invasive manner to achieve the same level of security;
3) whether the gains in security are worth the total costs of the security measure, including privacy costs and the opportunity costs of security-enhancing spending on health, education, poverty, and the environment; and
4) whether the costs are distributed fairly so that the increased security of the majority is not purchased by sacrificing the interests of a minority (Chandler, 2009, p.122).

Of particular relevance to the last consideration, Chandler warns,

> *"To the extent that data mining projects are based on a terrorist profile that specifies young, Muslim males of Arab ethnic background, and to the extent that data mining creates a large number of false positives, this minority group will find itself more frequently flagged for further groundless investigation. … In this way, national security is pursued in a manner that reduces the security of a minority within the population. Not only does this reduce the security of individual members of the minority group, it may reduce overall national security" (Chandler, 2009, p. 137).*

Chandler (2009) cites alienation of the members of these groups, owing to the racial profiling and targeting, as a major cause of such reduced overall security.

Chandler advocates viewing the issue of security in a broader way so as to include "human security" and threats to "acquired values," in addition to security of the state (2009, p. 123). Looking at security through this lens brings both privacy and security under the same moral umbrella, rather than pitting one against the other.

The importance of this security debate notwithstanding, the exclusive, or arguably even the greatest, threat to information privacy no longer comes from governments; rather, corporate data miners, or *privacy merchants*, who stand to profit by selling large volumes of personal information, such as purchasing decisions and Internet surfing habits, to the highest bidder, pose at least an equal, if not greater, privacy risk (Etzioni, 2012). Because it is easy for consumers online to shop around, they have a lot of choices and options, which makes the virtual commercial world especially competitive. Turnaround times are short and change happens quickly—speed and creativity is the order of the day. The fast pace and intense competition on the Internet encourages hypercompetitive behavior, which sometimes leads to decisions and actions that lack a full understanding of the ramifications, ethical or otherwise. Another aggravating factor is that, in many instances, given the transborder, cross-jurisdictional nature of the *e-vironment*, it can be challenging for e-businesses to remain adequately *au fait* with all applicable privacy laws and requirements. These challenges are especially acute for small e-businesses, which are increasingly omnipresent on the Web because low start-up and marketing costs, easy access to markets around the world, and the comparatively low cost of maintaining a corporate Web site create attractive, low-risk business prospects for new entrepreneurs with limited resources. Not surprisingly, therefore, it is relatively common for such start-up businesses to have privacy policies and ethical insight that lag well behind the power curve of innovation, development and deployment of new products and services. It is also common for the absence of a compelling business case to combine with deficient legislative incentives to render privacy protection far closer to the bottom, rather than the top, of the business priority list. In fact, typically the privacy regime exercised by small online businesses—to the extent that one is exercised at all—is heavily

dependent on the values, ethics, intuition and usually rather limited knowledge of privacy issues of one or two individuals—i.e., the corporate leaders and/or owners (Stevens, 2010).

There are also, however, far more deliberate threats to privacy stemming from what might be described as predatory behavior, motivated by greed or other narcissistic tendencies and enabled by disregard to ethicality and responsibility. As we process emails, do online banking and make e-purchases, or even as we merely surf the Web, we generate digital footprints. Many Web site developers or managers, operating on behalf of online vendors or ISPs, engage in covert data collection activities such as remotely depositing "cookies" on our computers and smart devices, tracking our digital footprints, or employing other data mining techniques to monitor and track online searches, browsing habits and personal interests associated with a particular device and location (Shade 2008). Drawing from Stoddart's annual report, Shade notes that the personal information collected through the use of search engines and data mining techniques "can be collected and stored to create detailed profiles of user tastes and preferences in shopping, reading, and other habits, all of great value to corporations that rely on mass marketing" (2008, p.85). One of the primary uses of this gathered data is to help vendors more effectively "tailor" their marketing activities to specific audiences and thereby increase advertising efficiency and, ultimately, sales and profit. All this data manipulation and the vast processing and storage capacity that it requires has been made possible largely due to advances in both computing technology and data transport technology—the latter including the availability of once-unimaginable bandwidth, partly owing to the advent of fibre optics—and the sophisticated software applications that the new technologies allow. Stoddart has pointed out that children and youth are especially vulnerable to privacy threats posed by their Web surfing activities and the associated data mining by

marketers, who are using increasingly stealthy techniques. This "raises important ethical issues about children's rights to privacy and freedom of expression" (Shade, 2008, p. 85). Simon Davies (1997) astutely observes that over the course of little more than a generation, we have seen privacy gradually transform from an issue of ethicality, social values and human necessities and rights to one of strictly defined legal and consumer rights.

What is more, there is no evidence to suggest this trend is tapering off; in fact, quite the contrary—these activities continue to be on the rise, and many of these types of data mining activities are invisible to users, who have not consented to having their personal information thus collected and exploited. To be fair, in a number of instances the option is explicitly offered for the user to opt out of such data mining and usage; however, at least as frequently, users are not made aware of this option being available, if it even is available. Even when they are aware, users often "volunteer" to forfeit some degree of privacy because it is required in order to receive a perceived benefit. An example of this is surrendering personal information in order to gain access to a Web site, to use an online service, to make an online purchase, or to seize an opportunity to win a prize of some sort. Davies refers to this phenomenon as "the illusion of voluntariness" (1997, p. 142). The proverbial silver lining, insofar as there is one, is that sometimes the personal information provided—identity, location, age, income, et cetera—can be false without consequence to the user, which gives the user the option of answering truthfully or not (e.g., entering a false pseudonym, age or location). However, this requires some knowledgeable discernment on the part of the user as well as a willingness to answer dishonestly.

To cite one high-profile example of personal data mining and distribution, Facebook "Beacon" was launched in 2007 as an advanced advertising system that tracked certain online

activities of Facebook users on over 40 participating Web sites outside of Facebook. It then forwarded details of these activities—including, online purchases, subscriptions for services, additions to a wish list—to Facebook "friends," in some instances despite the original user having explicitly opted out (the default was opt in) or not even being logged in to Facebook, and in most instances completely unbeknownst to the user. The privacy violation and potential for embarrassment (and, in some instances, spoiled gift surprises) was so great, as was public outrage, that Facebook faced a class action lawsuit, which ultimately ended in Facebook's agreeing to pay out $9.5 million, more than $6 million of which was allocated to create a non-profit foundation intended to fund projects, initiatives and grants aimed at promoting online privacy, as well as safety and security (Perez, 2007, November 30; Brodkin, 2009, December 8; Kravets, 2010, March 17).

Another well publicized example of privacy invasion over the Internet is the "Google Buzz" case. In 2010 Google Inc. rolled out an online service called Google Buzz, which gave "Buzz friends" the ability to view and monitor the contacts of another account holder. As a consequence, relationships that the user had intended to be kept private—such as with psychologists, psychiatrists, lawyers and certain others—were publicly disclosed. The service used a default opt-in approach that in some instances failed to allow the primary user the ability to opt-out before damage from privacy violations had already occurred. As one writer put it, "the biggest problem with Buzz was Google's utter ham-handedness with privacy, which led to publishing members' profile data without permission—including their contact lists—and ultimately to an $8.5 million civil suit and an FTC-imposed independent privacy review board" (Koetsier, 2013, May 27). Google Buzz was later shut down.

Most recently, during the week of 21 October 2013, Bell Canada announced that it was planning to put in place a new monitoring and profiling regimen that would significantly expand the company's use of the information it gathers on its several million customers. The new regime would facilitate tracking of customer locations, media habits, search terms, Web-site interests and activities, and application usage, and would extend to essentially all media and communications activity, including which television programs are watched and what phone calls are made. The gathered data would be correlated with demographic and other information to enable detailed consumer profiling and targeted advertising. Every customer would be targeted and profiled unless they opted out—the opt-in status would be the default position. In addition, Bell acknowledged that it would be selling its data to marketing companies and other businesses, raising further privacy concerns. This development prompted Canada's Privacy Commissioner to undertake an investigation regarding the lawfulness and potential impacts of these plans (Geist, 2013).[3]

2.4 Mitigating Considerations

For the sake of balance and completeness it is important to note that, despite the challenges to privacy posed by many new technologies in common use, some technological advances have actually served to *increase* privacy, while still others have the as-yet-untapped *potential* to increase privacy. To cite one example, advances in telephone switching technology enabled a move from "operator-assisted" calling, where a caller had to ask a human "operator" to connect him with another named individual, to automated switching, which allowed direct dialing to a specific phone number without having to disclose (at least

[3] The results of the investigation were pending at the time of writing.

not to an operator) to whom you wished to speak and when. Further advances in communications technology in the 1960s enabled a mass move from "shared" service or "party line" service—wherein two or more households shared a common phone number—to the ubiquitous use of private, separate lines for each household. Further to the benefit of eliminating disturbances from phone calls intended for another household (barring "wrong numbers"), the introduction of private lines precluded the possibility of a party line co-subscriber listening in to another's calls, thereby significantly increasing privacy from the previous regimen. The even more recent introduction of *digital* technology has enabled further conveniences, including privacy enhancing services such as "caller i.d." or "caller display," as well as the ability to "block" certain callers; although, on the downside, the same technology also allows a caller to block her own identity from being revealed, which, while enhancing the caller's privacy, detracts from the recipient's ability to identify the caller and, hence, compromises her own privacy, as well as security.

Directing our attention to the Internet, several privacy enhancing technologies (PETs) have come to the fore in recent years. Some examples include: encryption, which helps ensure confidentiality and security by rendering the data unintelligible to unauthorized recipients; software to create audit trails of who accessed what information; and digital signatures, which include three features: *authentication*, to confirm that the person who sends a communication is actually the person she purports to be, thereby avoiding impersonation; *integrity*, to verify that the data is not corrupted or modified; and *non-repudiation*, to ensure that a sent message cannot be renounced or denied. There has also been increased pressure on commercial Web-site managers for greater transparency regarding their collection, usage, storage and sharing of personal information. Consequently, there has been an increase in the appearance and

comprehensiveness of policy statements on various commercial Web sites; although, these statements tend to be verbose, complex and legalistic, and of limited utility to most users.

Finally, there have been numerous developments regarding both legislation and its enforcement. Some of these developments are discussed later in this thesis. However, it would seem appropriate and useful at this juncture to note Davies's observation that, "While there are … more codes, conventions, and laws in place than ever before, more data on more people is being collected by more powerful systems and for more purposes than at any other time in history" (1997, p. 144).

3. Why Does Privacy Matter?

Having provided some background and context on how technology and its application has impacted privacy, a logical next step is to address the questions, So what? Why does it matter? Why should we care about privacy and technology's impacts on it? It is these sorts of questions that this chapter attempts to address by first highlighting a few of the more evident, immediate and direct risks of privacy invasion, and then presenting arguments that establish privacy as a psychological need, a social value and, finally, as a human right.

3.1 Risks

The storage of personal information in massive volumes and in almost countless databases, many of which are interconnected, makes it difficult if not impossible to ascertain, let alone to control or even influence, who has what personal information about oneself, how readily and widely it will be shared or made accessible, and how it will be used. We have already established that personal information is routinely sold to others for their marketing and other uses without our consent or even our knowledge. But this is just the proverbial tip of the iceberg. The following are but a very few examples of real and potential immediate consequences from online privacy invasion.

Unauthorized access to, or disclosure of, health-related information, including personal medical conditions and treatments or derivative information, can impact medical insurance coverage or even employment opportunities. It can also result in the revelation of sexual preferences, habits or propensities and lead to severe embarrassment, discrimination, alienation, and/or a sense of having been violated. For example, according to McFarland,

"if it becomes known that a person has a history of mental illness, that person could be harassed and shunned by neighbors. The insensitive remarks and behavior of others can cause the person serious distress and embarrassment. Because of prejudice and discrimination, a mentally ill person who is quite capable of living a normal, productive life can be denied housing, employment and other basic needs" (2012, p. 1).

Another example is the revelation of an arrest. Even in the absence of any convictions, a person who has been arrested, even if completely innocent, may be shunned, discriminated against or subjected to harassment. He is also far less likely to be hired, even if any charges had been dropped or in cases of complete acquittal (McFarland, 2012).

Employment actions are also impacted by online research conducted by employers, recruiters and human-resources professionals, who routinely use search engines, such as Google, and/or social media Web sites (e.g., Facebook, MySpace, LinkedIn, Twitter) to check out the online behaviour of, and references to, a prospective employee and to make hiring decisions based in part on their online findings. I personally know some astute individuals who use pseudonyms for their online blogs and other social media to avoid risking such scrutiny.

Non-consensual tracking of personal online activities, or, for that matter, activities in general, can reveal political or religious affiliations or leanings, sensitive personal views, preferences, plans or intentions, or personal affiliations with various groups, organizations or individuals—personal information that an individual might not wish to have publicly disclosed. Such intrusions can ultimately inhibit or restrict altogether legitimate activities, practices and pursuits for fear of external scrutiny and related consequences, and clearly

contravene a variety of fundamental rights and freedoms normally assured in a free and democratic society—e.g., the right to be secure against unreasonable search or seizure; the right to life, liberty and security; freedom of conscience and religion; freedom of thought, belief, opinion and expression; freedom of association and of peaceful assembly; freedom of movement; political freedom; and so on.

Documented personal information is sometimes incomplete, misleading, misrepresentative or simply wrong. Significant harm can occur when such information is publicly disclosed, as demonstrated earlier, even in instances where the disclosure is quite innocent or accidental. In other instances, however, stored personal information is accessed and used for malicious purposes. In some of the more acute instances, the disclosure of personal financial, business account, credit card or other sensitive information, such as passwords or social insurance numbers, can be used to commit fraud or identity theft and can cause tremendous financial losses and/or reputational damage. When, in certain contexts and without appropriate precautions, an agent discloses a person's address, travel habits, current or planned locations, and other identifying and revealing information, it can also create opportunities for harassment and/or lead to personal security risks, including physical harm, for the person whose privacy has been violated. Moreover, because of the serious potential consequences of the public disclosure of sensitive personal information, unauthorized access to or sharing of such information can also make the subjects of the information vulnerable to blackmail and extortion by unscrupulous individuals who come into its possession (McFarland, 2012). In a recent example, in December 2013, a "massive data breach" was reported, in which hackers stole user names and passwords associated with nearly two million accounts at Facebook, Google, Twitter, Yahoo and other online service providers through the

use of malicious key-logging software (Pagliery, 2013, December 4). At the time of this writing neither the intent of the data theft nor the extent of the damage had been determined.

In reference to security, privacy incursions carried out in the name of national security or law enforcement have led to several cases of unjust, even horrific, outcomes for the victims of those incursions. The Maher Arar case is probably the best known recent example of this. There have also been cases of innocent Canadians being included on various "no fly" lists, and it could happen to anyone unfortunate enough to have the same name as a person deemed suspicious by law enforcement entities (Shade, 2008). Looking globally, Michael McFarland points to the use, especially by totalitarian states over the past century, of sophisticated methods of surveillance to control citizens (2012). He cites, in particular, the Soviet Union, Communist China, Nazi Germany, Fascist Italy and white-run South Africa as countries that all employed covert and overt observation, interrogation, eavesdropping, reporting by neighbours and other means of data collection "to keep people in line," and that, where the surveillance failed to do so, "the data collected was used to identify, round up and punish elements of the population that were deemed dangerous" (McFarland, 2012, p. 5). Even today, in many places surveillance continues to be exercised "as an instrument of oppression" (McFarland, 2012, p. 5). One has to question whether such use could resurface in other places, as well.

McFarland notes that even democracies are not immune to such surveillance, citing the United States, "where freedom is such an important part of the national ethos," as an example. He observes that "the FBI, the CIA, the National Security Agency (NSA) and the armed forces have frequently kept dossiers on dissidents" (2012, p. 5). In particular, he highlights privacy invasions perpetrated by the U.S. Nixon administration in the early 1970s

and the Clinton administration in 1996, in each instance targeting the President's political opponents.

McFarland also speaks of developments following the terrorist events of September 11, 2001, observing that, "there has been even greater urgency in the government's efforts to monitor the activities and communications of people, both foreigners and its own citizens, in order to identify and prevent terrorist threats" (2012, p. 6). He refers to the enactment of the *Patriot Act* and notes that it "greatly expanded the (U.S.) government's authority to intercept electronic communications, such as emails and phone calls," and adds that, as a result, government agencies have been continually bolstering their capabilities to monitor private activities and communications, including those of their own citizens (McFarland, 2012, p. 6). He suggests that the mere knowledge of this can have a "chilling effect on political freedom" and can hamper society's openness to innovation and dissent (McFarland, 2012, p. 6). McFarland concedes, however, that governments require certain personal information to govern effectively and to protect the security of their citizens, but also points out that citizens nevertheless need to be protected from "the overzealous or malicious use of that information, especially by governments that, in this age, have enormous bureaucratic and technological power to gather and use the information" (McFarland, 2012, p. 7).

The above notwithstanding, many concerns and arguments could be, and have been, raised in connection with *excessive* privacy and the risks that it poses. Some might argue that too much privacy, particularly privacy *protection*, can put women at greater risk of domestic violence and abuse. Others might argue that too much privacy can facilitate the planning and execution of crimes and acts of terrorism, while concurrently impeding national security and law enforcement agencies from *fighting* crime and terrorism. Still others might point out the

cost to the commercial world and the global economy of their being overly restricted in terms of collecting and using personal information. However, despite the prima facie validity of these concerns, it is important to compare these risks and costs against those associated with deficient privacy. It is also important to point out that privacy advocates, certainly for the most part, seek the realization of optimum levels and modalities of privacy through: 1) the systemic recognition and protection of privacy as a human and societal need, value and right, and, 2) the appropriate balancing of privacy considerations with other, sometimes competing, needs, values and rights.

3.2 Privacy as a Psychological Need

The nature and scope of what is deemed to constitute *privacy*, the extent to which it is valued, and the ways that it is protected within different cultures appears to vary considerably (Rachels, 1975; Westin, 1967). However, the desire for privacy appears to be ubiquitous, instinctive and, according to research by legal scholar Alan Westin (1967), not limited to humans. Hence, one can reasonably conjecture that privacy, although manifested in various ways through an assortment of individual behaviours and social contracts, is naturally embedded in the human psyche. It can also be argued that the concept of privacy is innate to humans and even to other living beings.

Referencing the work of others on the subject of privacy, Chandler notes, "Privacy is said either to promote or to be a necessary component of human interests of inherent value such as human dignity, autonomy, individuality, liberty, and social intimacy" (2009, p. 124). Adam Moore asserts that, "Privacy ... is an essential part of human flourishing or well being"

(Moore, cited in DeCew, 2013). Charles Fried wrote, in 1970, that "privacy allows one the freedom to define one's relations with others and to define oneself. In this way, privacy is also closely connected with respect and self-respect" (Fried, cited in DeCew, 2013). Closely related to this, privacy helps us to establish self-concept and personal identity, both as independent individuals and as members of society. As McFarland aptly describes it,

> *"A normal person's social life … (encompasses) many different roles and relationships. Each requires a different persona, a different face. This does not necessarily entail deception, only that different aspects of the person are revealed in different roles. Control over personal information and how and to whom it is revealed, therefore, play an important part in one's ability to choose and realize one's place in society" (2012, p. 2).*

Deborah Johnson (2009), offering a rather Kantian perspective, observes that viewing individuals as autonomous beings, who are ends in and of themselves, requires allowing them to live as they choose, within limits, and that this includes their exercising choice over their human relationships; thus, since information mediates relationships, if people cannot control who has what information about themselves, their autonomy is diminished.

Fried (1970) argues that privacy is fundamental to one's development as an individual with a moral and social personality and who is able to form intimate relationships that involve respect, trust, friendship and love. In the absence of privacy that allows people to share deeply personal or highly sensitive thoughts, feelings and information without apprehension about disclosure to the larger community, intimate relationships are not possible (Fried, 1970; Solove, 2008). A husband and wife, for example, will behave differently in public or in the presence of a third party than when they are alone (Rachels, 1975). Julie Inness (1992) reiterates this view, stating that privacy, in enabling the sharing of intimate information and

engagement in private activities with confidentiality, allows one to fulfill one's needs of loving and caring for others. Privacy also enables an individual to control, to some extent, *who* is in a social relationship with that individual, and the level of intimacy of that relationship (Fried, 1970; Solove, 2008). Quoting James Rachels, Jason Millar submits that "our ability to control who has access to us, and who knows what about us, allows us to maintain the variety of relationships with other people that we want to have," and that is "one of the most important reasons why we value privacy" (Rachels, cited by Millar, 2009, p. 108).

We have established, therefore, that privacy aids self-esteem, self-concept, autonomy, self-actualization and control over one's destiny, and that it is a prerequisite for intimacy and close personal relationships. However, even beyond this, privacy is essential to maintain *all* types of social relationships, not only intimate or close personal ones (Rachels, 1975), and it holds instrumental value for society at a broader level. As an example, much of what a patient tells her doctor or therapist would not be something that she would want others to know. Such a relationship is privileged and requires a certain level of openness and trust to be functional; however, such openness and trust cannot occur without some reasonable degree of assurance and confidence that privacy will be maintained.

Conversely, a threat to privacy constitutes a threat to our very integrity as persons (Fried, 1970). Surveillance and the invasion of privacy in general is an affront to human dignity (Bloustein, 1964), and it reduces self-determination; it "impairs aspects of individuality that are, or should be, protected in a free and democratic society" (Uteck, 2009, p. 90). Lack of privacy makes everything public and opens the domestic sphere to surveillance, complete scrutiny and intrusion by the state (Allen, 1988). "A person who is

completely subject to public scrutiny will lose dignity, autonomy, individuality, and liberty as a result of the sometimes strong pressure to conform to public expectations" (Chandler, 2009, p. 124). Westin claims, "the deliberate penetration of the individual's protective shell, his psychological armor, would leave him naked to ridicule and shame and would put him under the control of those who know his secrets" (1967, p. 32). Thus, privacy is also essential for freedom from external interference, scrutiny and pressure, as well as for psychological security. "To lose control of personal information is to lose control of who we are and who we can be in relation to the rest of society. … If (a person's) every appearance, action, word and thought … is captured and posted on a social network visible to the rest of the world, they lose that freedom to be themselves" (McFarland, 2012, p. 4).

Our thoughts, once articulated, become information. If articulated in confidence those thoughts become *personal* information. Such personal information is often particularly sensitive because it is preliminary, unevaluated, unedited, and still undergoing formulation. Moreover, it has not yet been acted upon, and it allows us to "test the waters," as it were, regarding potential courses of action, or merely to discern and reflect on our personal convictions. When the articulation or expression of those thoughts is denied out of concern over privacy, it limits, even stifles, full self-exploration, self-awareness and self-development, as well as freedom.

Offering a contrasting perspective, Richard Posner (1981) suggests that privacy is usually used to mislead or manipulate others, and that its value is, therefore, overrated. I disagree. If, for example, one considers privacy within the context of activities that are of a highly personal nature or the expression of intimate or sensitive views, beliefs or feelings, it is

not a stretch to accept that privacy as a concept is reasonable, appropriate and, frankly, essential, and that its primary utility does not lie in manipulating or misleading others. In such a context any effort to control privacy is motivated merely by the natural propensity to maintain a certain level of comfort with respect to sharing with others information that is of an inherently personal, intimate or sensitive nature. In other instances, admittedly there may be some degree of impression "management" at play; however, the agent is often simply exercising their freedom to choose what personal information is being shared, how, when and with whom. Privacy, particularly *information* privacy, is about managing the disclosure of one's personal information and, concurrently, one's relationships with others, as well as with oneself. This is markedly different than attempting to mislead or manipulate others.

3.3 Privacy as a Social Value

Privacy is sometimes viewed as inherently asocial or even antisocial. I would argue quite the contrary, however, that privacy is necessarily social by its very nature, and that it is, in fact, a social value. Gregory Walters notes, "… comparative anthropological and social scientific studies … reveal the important role of privacy as a social value in all human associations," adding that privacy is essential in order for us to "develop our full humanity" (2001, p. 169). Deborah Johnson (2009) considers privacy a social good that is essential for democracy. Valerie Steeves contends that privacy focuses exclusively on one aspect of human relationship management—one which she describes as "a dynamic process of negotiating personal boundaries in intersubjective relations" (2009, p. 193). Steeves also borrows from Westin, who, in turn, draws on works by Edward Hall and Robert Ardrey, in writing,

> *"privacy is rooted in human evolution and … privacy norms are present 'in virtually every society.' Although these norms vary from culture to culture, as they are contextual and based, in part, on how others will respond to any given personal information in relation to an individual, 'a complex but well-understood etiquette of privacy is part of [every] social scenario.' From this perspective, then, privacy is inherently social—it is part of the way in which social beings interact" (Steeves, 2009, p. 196).*

Steeves also observes that "privacy is … dependent … on the negotiated interaction between social actors … the social negotiation of a desired boundary between self and other; it cannot be achieved by the individual in isolation" (2009, p. 207).

Westin highlights the importance of privacy to social democracy when he observes,

> *"Just as a social balance favoring disclosure and surveillance over privacy is a functional necessity for totalitarian systems, so a balance that ensures strong citadels of individual and group privacy and limits both disclosure and surveillance is a prerequisite for liberal democratic societies. The democratic society relies on publicity as a control over government, and on privacy as a shield for group and individual life" (1967, p. 24).*

Privacy as a concept and social construct has existed since the days of Aristotle, as indicated earlier, and well before. It can be argued that it has also existed as a social *value* equally long, especially given a natural propensity for humans, as well as non-humans, to seek it in any of its various forms and to protect it, both individually and collectively. There is an extensive list of devices that humans have relied upon to enhance and protect privacy—walls, fences, doors, partitions, privacy glass, "no trespassing" signs, and even clothes are but a small handful of them. The major attraction of telephones with dials versus those requiring operator assistance, and of private lines over shared service lines, was the added privacy

afforded the user. The notion that privacy has essentially always been a social value is not surprising when one considers the vast array of its previously mentioned benefits to social interaction, communication, relationships, innovation, and, thus, its value to society overall.

What about in today's globalized world—is privacy still upheld as a social value in a meaningful way? There are those that stand to profit by convincing us that privacy no longer matters to people, and some who attempt to manipulate public views accordingly. It is not surprising, therefore, that there is a common perception—a misconception—that people, especially those of the younger generation, who are the most prevalent users of social media and most inclined to share personal information about themselves on social networking sites, don't care about privacy. The reality, however, is that they do care, and very much. Broad consultation and research by the Office of the Privacy Commissioner of Canada (OPC), as well as surveys conducted by others, indicate that, although social norms are evolving and we, as a society, have become more open in many ways, people, regardless of age, continue to value their privacy. In fact, they cherish it (OPC, 2013a).

Survey results also indicate that there is a continuing increase in concern over privacy, especially over its violation (Davies, 1997). In 1976 a Harris poll revealed that 47% of Americans surveyed were "very concerned" or "somewhat concerned" about privacy. In 1983, just seven years later, this figure had increased to 76%, and by 1995 it had reached 82%. A Yankelovich poll also taken in the 1990s revealed that 90% of Americans were in favour of legislation to protect them against privacy invasion by businesses. A mid-'90s Morgan Gallup poll in Australia showed that privacy ranked second in importance, topped only by education (Davies, 1997). Other evidence of the value of *online* privacy, in particular, arose from a substantial survey conducted in 2002 among University of Singapore students.

The survey indicated that guaranteeing online privacy—even just in terms of non-sharing of personal information with third parties—had such universal appeal that it could spawn a multi-billion-dollar industry in the United States alone (Hann et al, 2002).

An Ekos Research Associates survey conducted in March 2006 for the OPC indicated that Canadians are highly concerned about the privacy of their personal information, and that 7 out of 10 people feel it is more at risk than it once was. A reported two-thirds of those polled cited privacy as "one of the most important issues facing our country in the next 10 years" (Shade, 2008, p. 81). The survey also found that the majority of Canadians felt that updated privacy legislation was in order, owing to technological developments, and that they wanted the ability to exercise control over their personal information and tracking devices. Interestingly, but perhaps not surprisingly, Canadians generally expressed more privacy concerns about the impact of certain recent U.S. legislation (i.e., the *Patriot Act*) than about any Canadian legislation (Shade, 2008).

The young users of social media are particularly concerned about their reputations, and they generally "share" the information that they do online on the assumption that the Web site being used is secure and that they can control access to that information. In general, people want to manage who has access to what personal information about themselves, and this applies as much to the digital domain as anywhere. The complaints that have been brought against certain social networking service providers over changes to their services that impacted users' ability to control their privacy risk provide clear evidence of this (OPC, 2010).

Interestingly, however, there appears to be a common perception of privacy protection that is relatively narrow in scope, i.e., that it comprises essentially "a set of technical rules governing the handling of data" (Davies, 1997, p. 144). Simon Davies notes a "shift in the perception of privacy and privacy invasion" and "fundamental changes (that) have taken place in society's approach to traditional privacy issues" (1997, p. 144). He identifies five major factors underlying this change. The first is a shift in focus from *privacy* protection to *data* protection. This is attributable to the relative ease with which laws, regulations, rules, directives and various policy instruments can be formulated and implemented to govern how personal data is handled. A focus on data protection also appears to be quite effective in readily appeasing public concerns over loss of privacy. However, citing shortfalls in this approach, Davies observes,

> *"One of the broadest deficiencies is that they are seldom privacy laws. They are information laws, protecting data before people. Instead of being concerned with the full range of privacy and surveillance issues, they deal only with the way personal data is collected, stored, used and accessed … it would be a mistake to assume that they will address the most pressing privacy problems" (1997, p. 144).*

The second factor is a transformation of traditional skeptics into "partners" by inviting broad participation in community activities that have either direct or indirect privacy implications. Neighbourhood Watch and "Crime-stoppers" initiatives would be two examples. Third is the "illusion of voluntariness," which stems from a trend toward including a "voluntary" component in many surveillance schemes and, in the process, helping to quell public concern over surveillance (Davies, 1997, p. 144). Calls for voluntary DNA testing to help rule out certain potential crime suspects is one example. Another is the taking on of a national ID card

to facilitate receipt of universal government services. In the former instance, the donor has just surrendered his genetic code; in the latter, the card bearer has facilitated the mass storage and ready availability to any government entity of all personal information ranging from medical records and other health-related information to parking tickets to driving infractions to tax records to toll highway usage—including date, time and location—to international travel, and so forth. To be truly voluntary, however, there must be no pressure to volunteer; but when one does not volunteer for DNA screening, for example, one becomes even more of a suspect because of the appearance of having something to hide, and if one does not sign up for the national ID card, the decliner is likely to suffer repercussions in terms of reduced or forfeited services or other inconveniences. The fourth major factor is the commoditization of privacy rights, where privacy protection has become an afterthought and is seen as an added expense to industry such that businesses offer limited privacy to customers as an option for which the latter pays. An example of this is caller ID—throughout most of the time that society has enjoyed the telephone, it has been the responsibility, and discretion, of the caller to identify herself; however, the advent of technological features such as caller ID and ID blocking have made it optional, at added cost, for the caller to preserve the anonymity and associated security (from the caller's perspective) that was once a given. Fifth, and finally, the public interest argument is used almost routinely to justify various encroachments on privacy, whether or not the public interest is, in fact, truly best served by said encroachment. These trends have changed, and are continuing to change, the face of privacy (Davies, 1997), but the legitimacy and significance of privacy as a social value remain unchanged.

Curiously, while privacy is widely shown and acknowledged to be a great concern, privacy advocacy is at an all-time low (Davies, 1997). This raises questions like, Is privacy

something that we knowingly have to trade for goods, services and conveniences in today's high-tech world? Have we become so resigned to diminished privacy that many of us now simply accept it as part of the cost of doing business—of living—in the modern era? Have we all but given up on privacy and its protection because we see it as a futile endeavour in the face of today's technological environment and consumerism? Helping to shed light on these questions, the aforementioned mid-'90s Australian Morgan Gallup poll found that 7 out of 10 respondents felt that privacy is extinct, owing to the perception that their government is effectively omniscient as regards its citizens. The 1995 U.S. Harris poll results indicated that 80 percent of Americans felt they had lost all control over their personal information. More generally, residents of Western industrialized nations reportedly "feel powerless to defend themselves against intrusive practices" (Davies, 1997, p. 147). The indicated pessimism notwithstanding, however, privacy clearly remains a strong social value.

3.4 Privacy as a Right

This section takes a cursory look at the issue of fundamental rights within the context of privacy. It does not limit itself specifically to human rights, legal rights, civil rights or moral rights. Rather, it is intended to serve as a window into the broad realm of rights writ large in relation to privacy by providing a small sample of the concepts and views that have been articulated on the subject.

Jan Garrett (2002) asserts that, "Privacy rights have both protective and enabling functions." According to Garrett, the *protective* functions include the following:

1) to prevent others from obtaining information that would expose persons to shame, ridicule, embarrassment, blackmail, or other harm;

2) to prevent others from interfering with our plans simply because they have a different conception of the good; and
3) to prevent persons from accidentally harming their own reputations.

He notes that these protective functions are required because of certain people's intolerance of, or disrespect for, religious or philosophical differences or certain sexual orientations, and acknowledges that some people are inclined to abuse information they have about others, including to dominate others for purposes of economic or political gain.

As regards *enabling* functions, Garrett maintains that a right to privacy:

1) makes possible intimate relationships that would not be possible without privacy protections;
2) makes possible the existence of certain important professional relations (e.g., doctor/patient, lawyer/client, clergy/parishioner);
3) makes it possible for persons to sustain multiple social roles (e.g., a corporate manager may want, in his non-corporate role, to support political causes that are unpopular among his management cadre); and
4) gives persons control over how they present themselves to society.

With a view specifically toward *human* rights, from which other rights arguably must stem, The Open University (2011) Web site points out that, "Privacy has long been recognised as one of the important human rights and this is reflected in religion and history. There are, for example, references to privacy in the Qur'an, the Bible and Jewish law. Privacy was also protected in classical Greece and ancient China." Walters asserts that, "The justificatory ground of human rights is a moral principle that establishes that all humans are

equally entitled to have the necessary conditions of freedom and well-being in order to fulfil the general needs of human agency" (Walters, 2001, p. 37). Specifically in relation to privacy, Walters eloquently presents a Gewirthian perspective (discussed later in this thesis) in arguing that privacy is indeed a human right precisely because it satisfies the criterion of being a necessary condition of both freedom and well-being. Consistent with this perspective, Gus Hosein argues that privacy is a prerequisite for human dignity and for fulfilling "the core objective of human rights," adding that "privacy can be seen as a core protection of individual autonomy and human agency" (Hosein, cited by Shade, 2008, p.82). The 1980 Williams Commission Report (which served as the foundation for the establishment of the Ontario Freedom of Information and Protection of Privacy Act (FIPPA)) also expressed the importance of privacy in human rights language, stating that privacy "is linked to fundamental concerns for the preservation of human dignity and personal freedom" (Lawson & O'Donoghue, 2009, pp. 26-27). Likewise, the Organisation for Economic Co-operation and Development (OECD) considers acts such as "the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data" to constitute "violations of fundamental human rights" (OECD Web site, 2013b). Valerie Steeves sees privacy as both a social value and a human right, and argues that it is essential to the democratic process (Steeves, cited by Shade, 2008). The report of the Review Group on Intelligence and Communications Technology identified six goals to be pursued by the U.S. to deal with the "rapidly changing world"; one of these was "protecting the right to privacy" (cited in NSA review panel findings: Liberty and Security in a Changing World, 2013, December 18). The report noted, "The right to privacy is essential to a free and self-governing society. The rise of modern technologies makes it all the more important that democratic

nations respect people's fundamental right to privacy, which is a defining part of individual security and personal liberty" (cited in NSA review panel findings: Liberty and Security in a Changing World, 2013, December 18).

Rachels (1975) argues that, because privacy is a prerequisite to maintaining social relationships, it should be considered a distinctive right. Lawrence Lessig (2006) feels strongly that individuals should be able to control information about themselves and suggests that the protection of privacy would be more viable and stronger if people conceived of the right as a property right. McFarland attempts to resolve the privacy rights debate by pointing out that, "even if privacy is not in itself a fundamental right, it is necessary to protect other fundamental rights" (2012, p. 1). An example of this would be, as some have argued, that privacy, while distinct from liberty, is essential for protecting liberty, and even inherent in the *right* to liberty.

Jean L. Cohen (2002) appears to take inspiration from Habermas and other European philosophers in presenting a constructivist defence of privacy, arguing that privacy rights protect personal autonomy and that a constitutionally protected right to privacy is indispensable for a modern conception of reason as well as autonomy. William Parent (1983) and others (Henkin, Thomson, Gavison, Bork) have pointed out that constitutional right to privacy cases tend to focus exclusively on liberty, and yet, the right to a secret ballot, which exists in virtually all democratic jurisdictions, is clearly a form of privacy right. One could counter, perhaps, with the contention that the right to a secret ballot is based on the freedom to vote without concern for external scrutiny—hence, a liberty-based right—but, even so, I would argue, the concern is based on external interference or repercussions arising from an unintended awareness by others of our personal and potentially sensitive beliefs, desires,

convictions and preferences—ergo, a loss of privacy—and, hence, the right to a secret ballot is indeed, as Parent claims, a form of privacy right.

An Israeli law school treatise on the subject of privacy "in the digital environment," submits that the "right to privacy should be seen as an independent right that deserves legal protection in itself," (Onn et al., 2005, p. 3) and, accordingly, has offered the following definition for a proposed *right to privacy*:

> *"The right to privacy is our right to keep a domain around us, which includes all those things that are part of us, such as our body, home, property, thoughts, feelings, secrets and identity. The right to privacy gives us the ability to choose which parts in this domain can be accessed by others, and to control the extent, manner and timing of the use of those parts we choose to disclose" (Onn et al., 2005, p. 12).*

U.S. Supreme Court Justice Louis Brandeis (1890) became the first U.S. jurist to define privacy as a legal right. In the Harvard Law Review article *The Right to Privacy* Brandeis and co-author Samuel Warren (1890) make reference to the sanctity of private and domestic life and speak of the invasion of privacy as an evil. Moreover, they advocate for strengthened legal protection and criminal sanctions against invasions of privacy. It is important to note, however, that they also speak in favour of balance to ensure that society's needs, as well as the needs of the individual, are met. Westin (1967), like Brandeis, contends that privacy rights have to be balanced with the ability of government to conduct surveillance in order to protect democratic processes, and has openly supported the highly controversial U.S. *Patriot Act*, declaring it "a justified piece of legislation" (Westin, cited by Fox, 2013, February 22). Also favouring a balanced approach, McFarland argues that privacy cannot be absolute and that governments require "a certain amount of information on its citizens in

order to govern efficiently, provide for their security and distribute benefits and obligations fairly," while also conceding that the "obligation to share information for the common good does not always take precedence over the right to privacy. Rather the two must be held in balance, for both are necessary for a fully human life" (McFarland, 2012, p. 7). Walters (2001) also acknowledges that human rights are not absolute and that it is sometimes justified to infringe on certain individual rights, including privacy, to protect the rights of others, particularly where so doing is in the clear interest of the public or where a greater good case can be made on grounds that are ethically sound (such as on the basis of Gewirth's Principle of Generic Consistency).

In closing, privacy supports freedom by allowing a person to escape, at least to some extent, the watchful eye and scrutiny of the public, to act without fear of others' awareness or judgement, or of any associated consequences. Privacy thus lessens self-imposed restrictions and gives one the liberty to enjoy a greater range of activities and to self-actualize in ways that would not otherwise be possible. It is also fundamental to the human psyche, integral to social interaction, and essential for individual and societal functioning and well-being. I submit, therefore, that even if privacy is, in effect, addressed by rights otherwise conferred, its fundamentality to the human experience is such that it warrants being universally accepted, declared and enshrined as a right in and of itself, even if not absolute and inalienable. To that end, the addition of some such explicit wording to existing national charters might be a relatively straightforward way to effect such a change. An alternative approach would be to enact an independent charter or statute specifically to address privacy issues.[4]

[4] See the reference to *Charter of Privacy Rights* under "Canada" in the following chapter, for an example.

4. How Are We Responding?

To date, and in large part, the issue of privacy protection has been officially addressed through legislation at the federal level—and, in some instances, below—and the establishment of commissioners charged with overseeing compliance with that legislation as well as with undertaking initiatives to promote privacy through research, advocacy, partnering with counterparts in other jurisdictions, and submitting recommendations and challenges to their respective governments. There have also been international efforts aimed at establishing universal privacy rights frameworks of various sorts. Unofficially, however, advocacy groups, such as assorted civil liberties associations, Internet policy forums, and the Global Internet Liberty Campaign, have fought in favour of privacy by raising public awareness and lobbying against privacy-invasive corporate initiatives and legislative proposals, the latter typically associated with law enforcement, intelligence gathering and/or national security pursuits. It is worth noting that industry, while posing some of the greatest threats to privacy, has also developed products and services to help bolster privacy, particularly online privacy. This chapter highlights some of the more relevant of the above developments and initiatives.

4.1 Legislation

It is generally agreed that, certainly in most jurisdictions world-wide, the legal rights afforded citizens explicitly in terms of privacy are quite limited. Rather, to the extent that privacy has enjoyed protection under the law, it has largely been as a by-product of legislation targeting other issues, such as theft, assault and physical security, slander and libel, fraud, blackmail, embezzlement and, of course, individual liberties. In a number of instances some degree of privacy protection has been built into national constitutions. Conversely, in most of

these countries laws also exist that *limit* privacy by requiring constituents to compromise their privacy, such as when reporting earnings for income tax purposes.

If privacy is a legal right, then that imposes certain obligations on the state—or jurisdiction conferring that right—to respect, protect and promote that right. To date, privacy has not been universally established as a legal right per se and there is no universally accepted set of laws or edicts directly and explicitly relating to privacy. This is due, at least in part, to the breadth of the concept and to the challenges in defining what is private and worthy of legal protection, and in determining the extent to which, and the modalities by which, such protection should be afforded. Consequently, the legal protection of privacy afforded individuals, especially beyond that pertaining to the sanctity of one's home and real property, has been sketchy and fragmented. The most universal protection of privacy is conferred by Article 12 of the Universal Declaration of Human Rights, established by the United Nations (U.N.) General Assembly in 1948, which states the following:

> *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.*

Building on this UN declaration, certain aspects of privacy have been explicitly protected by law in dozens of countries, thereby effecting a limited regime of privacy legal rights within those particular jurisdictions; however, the vast majority of the afforded privacy protections has been based on the concept of *fair information principles*, developed in 1967 by Westin, and is focused on a relatively limited aspect of privacy, namely the protection and accuracy of personal information, and on the collection, use, handling, sharing and storage of that information. In only certain instances is consent by the person concerned required.

Exacerbating the legislative shortfall is the fact that the rate of advancement of information technology far exceeds that of any legislative process. This has led to what Steeves refers to as "the gap between the goal of data protection legislation and the reality of life in the surveillance society" (2009, p. 192).[5] Privacy legislation has had to adapt to developments in technology, but for the most part has been unable to keep up with the rapid pace of technological development and the ever-changing IT landscape, including the continual deployment of new data collection methods and the proliferation of privacy risks. In the international arena various efforts, such as the creation of the Asia Pacific Economic Cooperation (APEC) Privacy Framework, endorsed by APEC ministers in 2004, or the adoption of Privacy Principles earlier in 1980 by the OECD, have been undertaken to establish binding principles to protect personal information in recognition of the need to encourage and facilitate the unimpeded flow of information across a globalized environment, while concurrently upholding "fundamental human rights," including, in particular, privacy rights (OECD, 2013a). Not surprisingly, what amounts to a collage of policy and legislative solutions has enjoyed only limited success, as weak enforcement and inconsistent interpretation, application and rulings, combined with competing motivations, have hampered the effectiveness of many of these efforts.

The remainder of this section outlines some of the country-specific or regional legislative measures that have been taken in relation to privacy. It is important to note that this is not a comprehensive treatment of privacy-related legislation; rather, only select examples of particular significance to this thesis are provided herein.

[5] The term "data" in the preceding quote could easily be replaced with the word "privacy" and still hold true.

Canada

In Canada, as in many countries, legislated privacy protection is limited. Although Canada was one of the original signatories of the aforementioned Article 12 of the U.N. Declaration of Human Rights, and despite that there have been numerous policy debates and political discussions on the subject, privacy has never been formally established as a right within Canadian law. That having been said, privacy is nevertheless protected by multiple statutes—i.e., there is an array of legislation that *relates* to, and directly or indirectly protects, privacy. Canada's privacy-related legislative landscape is perhaps best described as "a patchwork of protections" (Shade, 2008, p. 83).

The *Canadian Charter of Rights and Freedoms* (1982) is the supreme authority in Canada's legislative hierarchy. It contains two sections (7 and 8) that provide limited and indirect protection of privacy. Section 7 guarantees "the right to life, liberty and security of the person," and pertains to privacy only insofar as it has been deemed, in certain instances, to preserve anonymity, a component of privacy (Lucock & Black, 2009). Section 8 of the Charter guarantees everyone "the right to be secure against unreasonable search or seizure." This provision has been interpreted to include unwarranted intrusion by the state and, in practice, is limited in application to instances where there is a reasonable expectation of privacy (Lucock & Black, 2009). These protections of privacy notwithstanding, the Charter fails to recognize privacy as a right per se, or to protect it in a broad or categorical way. Rather, privacy is addressed only tangentially, in a relatively piecemeal fashion and in limited contexts.

Another key statute is the *Privacy Act*. "The Privacy Act (1985) applies … to the federal public sector in relation to data collection, placing limitations on the collection, use,

disclosure, and disposal of personal information held by the federal government and federal agencies" (Shade, 2008, p. 83).[6] Information privacy legislation pertaining to the private or corporate sector was enacted fifteen years after the *Privacy Act* under the *Personal Information Protection and Electronic Documents Act (*PIPEDA, 2000) and deals with the collection, use, and disclosure of personal information, but only for the transaction of commercial activities (Shade, 2008, p. 83). One other piece of federal legislation particularly worthy of note is the *Canada Elections Act* (2000), whose sections 163 and 164 guarantee the anonymity or "secrecy" of a given voter's ballot selection.

Legislation also exists, however, at the provincial level to govern privacy protection by both public and private sector organizations. As reported by the OPC (2013b):

> *"Every province and territory has privacy legislation governing the collection, use and disclosure of personal information held by government agencies. … Oversight is through either an independent commissioner or ombudsman authorized to receive and investigate complaints.*
>
> *Several provinces have passed legislation to deal specifically with the collection, use and disclosure of personal health information by health care providers and other health care organizations.*
>
> *Several federal and provincial sector specific laws include provisions dealing with the protection of personal information. The federal Bank Act, for example, contains provisions regulating the use and disclosure of personal financial information by federally regulated financial institutions. Most provinces have legislation dealing with*

[6] Federal government institutions are also subject to Treasury Board policies and directives, as well as departmental policies, on personal information management practices.

consumer credit reporting. These acts typically impose an obligation on credit reporting agencies to ensure the accuracy of the information, place limits on the disclosure of the information and give consumers the right to have access to, and challenge the accuracy of, the information. Provincial laws governing credit unions typically have provisions dealing with the confidentiality of information relating to members' transactions. There are a large number of provincial acts that contain confidentiality provisions concerning personal information collected by professionals."

Four provinces—British Columbia, Manitoba, Newfoundland and Saskatchewan—have enacted legislation establishing statutory torts for wrongful invasion of privacy.

"Each one creates a right of action for invasions of privacy per se, without the necessity of the plaintiff proving any damage. Although 'privacy' is not defined in any of the Acts, every provincial privacy statute sets out various ways in which privacy may be invaded—eavesdropping, surveillance, wire-tapping, use of personal documents, and appropriation, to name a few" (Martin & Adam, 1994, p. 855).

In a curious recent (May 22, 2013) ruling, however, and despite the existence of a *statutory* law tort for invasion of privacy, the Supreme Court of British Columbia (B.C.) held that, "No *common* law tort of invasion or breach of privacy exists in British Columbia" (italics added; Hung & MacIsaac, 2013, June 17). This ruling serves to further obfuscate the legislative landscape regarding the protection of privacy.

In stark contrast to the B.C. development, on January 19, 2012, the Ontario Court of Appeal, in a historic decision, recognized a common law tort for the invasion of privacy—specifically, "intrusion upon seclusion," which consists of three elements:

1) intentional or reckless conduct on the part of the defendant,

2) an invasion of the plaintiff's private affairs without lawful justification, and

3) an invasion that a reasonable person would regard as highly offensive and that causes the plaintiff distress, humiliation or anguish (Hasselback, 2012, January 24).

"This decision has potentially significant implications, not just for individuals who may have invaded another person's private affairs, but for any organization that collects and/or uses personal health, financial and other information" (Dolman, Thomas & Bruschetta, 2012, January 23). It also "represents an important evolution in Canadian privacy law" (Wasser, 2013, February). The Ontario Superior Court had initially ruled that Ontario common law did not recognize a tort of invasion of privacy, and noted that privacy legislation in Canada provided "a balanced and carefully nuanced system for addressing privacy concerns" (Wasser, 2013, February). However, the recent Ontario Court of Appeal decision overturned the lower court's finding (Wasser, 2013). According to Lyndsay Wasser,

> *"A central rationale for the recognition of the new cause of action was the unprecedented power to capture and store vast amounts of personal information using modern technology. Over the past century, technological changes have included the invention of near-instant photography and the proliferation of newspapers. Today, highly sensitive personal information can be accessed with relative ease, including financial and health information as well as data related to individuals' whereabouts, communications, shopping habits and more. The appeal court determined that the common law must evolve in response to the modern technological environment" (2013, February).*

The court also acknowledged, however, that "the protection of privacy may give rise to competing claims, such as freedom of expression, which may trump privacy rights" (Wasser, 2013, February).

In addition to the legislation itself, there are formal bodies and mechanisms that have been established specifically with the aim of protecting and promoting privacy. These consist primarily of privacy commissioners and information commissioners at both the federal and provincial levels, whose mandates are to oversee compliance with relevant privacy protection and access-to-information legislation, as well as to promote privacy awareness and cooperation and a culture of respect for privacy. At the federal level, in particular, the OPC is charged with overseeing compliance with the *Privacy Act* and PIPEDA, as well as to encourage dialogue and promote education related to privacy within Canada and internationally. The OPC is also engaged in promoting common interpretations and standards to help achieve badly needed consistency across all jurisdictions—domestic and international—given that we operate in what has effectively become a single global information infrastructure.

For two federal organizations that are members of the Canadian security and intelligence community—i.e., the Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment Canada (CSEC)—there are additional scrutinizing mechanisms in place to ensure the lawfulness of their operations, particularly as regards non-invasion of privacy owing to the potentially intrusive nature of their mandates. CSIS is monitored by an independent external body known as the Security Intelligence Review Committee (SIRC), and CSEC's "watchdog" is the CSE Commissioner, who is a supernumerary or retired judge of a superior court and who has a staff to support him in carrying out his mandate. Both bodies report regularly to Parliament on their findings.

While the above-mentioned developments have taken place with the general intention and/or effect of better protecting privacy, one particular piece of legislation has been

introduced that has been deemed to further *challenge* privacy. Shortly after, and in direct response to, the infamous terrorist attack of September 11, 2001, the *Anti-terrorism Act* was created. This development prompted then Privacy Commissioner George Radwanski to write, "The fundamental human right of privacy in Canada is under assault as never before," and to express his concern that "we are on a path that may well lead to the permanent loss not only of privacy rights that we take for granted but also of important elements of freedom as we now know it" (Radwanski, cited in Shade, 2008, p.80). Radwanski contended that the government's new initiatives to collect and use personal information in the name of fighting terrorism might "establish a devastatingly dangerous new principle of acceptable privacy invasion" (Radwanski, cited in Shade, 2008, p.80). More recently, other bills were drafted that were deemed to further jeopardize privacy. These included bills to introduce "Lawful Access" legislation, aimed at helping the law enforcement and security and intelligence communities maintain their operational capabilities in the face, and wake, of rapidly evolving information technology, and a so-called "Online Surveillance Bill" (Bill C-30, 2012, February) to introduce a *Protecting Children from Internet Predators Act*; however, widespread opposition, particularly from privacy commissioners and civil liberties groups over the curtailing of privacy rights, resulted in their ultimate withdrawal. Exacerbating these concerns has been the establishment of free trade provisions that permit outsourcing of Canadian information by U.S. private corporations operating in Canada, thereby subjecting that information to U.S. legislation, including the highly controversial *Patriot Act* (Shade, 2008).

There was a legislative proposal to *enhance* privacy that was also unsuccessful. Because of its potential significance to privacy, however, it warrants elaboration herein. A 1997 House of Commons Standing Committee on Human Rights and the Status of Persons

with Disabilities was charged with seeking broad public input into some of the key privacy issues of the day, including genetic testing, smart cards, biometric encryption, and video surveillance. The Committee viewed privacy not only as data protection, but as a human right and a social value. In an initial report, the Committee, chaired by then Senator Sheila Finestone, wrote:

> "*Canadians see privacy not just as an individual right, but as part of our social or collective value system. … Canadians view privacy as far more than the right to be left alone, or to control who knows what about us. It is an essential part of the consensus that enables us not only to define what we do in our own space, but also to determine how we interact with others—either with trust, openness and a sense of freedom, or with distrust, fear, and a sense of insecurity*" (cited by Shade, 2008, p. 83).

In 2000 the Senate Committee proposed that a *Charter of Privacy Rights* be created to serve as a quasi-constitutional document that would provide an overarching legislative framework to protect privacy in general (Shade, 2008).

The privacy rights Charter was intended to go further than PIPEDA by establishing privacy rights in connection to the collection, use, and disclosure of personal information; physical privacy; freedom from surveillance; and freedom from the monitoring and interception of private communications. In effect, the Charter would serve as a sort of legislative umbrella that would set out the governing principles for privacy in Canada (Shade, 2008).

In 2001, the proposed privacy rights Charter, along with Senator Finestone's rationale behind it, was openly described as follows:

"(Senator Finestone) underlined that while privacy is a fundamental human right, it is not an absolute or inflexible right. Under section 1 of the Canadian Charter of Rights and Freedoms, it is subject to such reasonable legal limits as can be demonstrably justified in a free and democratic society. Senator Finestone explained that the bill is intended to set out an explicit legal right to privacy—something Canadian law does not currently contemplate—while giving effect to the principle that privacy is essential to an individual's dignity, integrity, autonomy, well-being and freedom, and to the full and meaningful exercise of human rights and freedoms. Senator Finestone noted that the bill would be paramount over other ordinary legislation and would necessitate a review of existing, as well as all new, federal legislation to ensure compliance with the bill" (cited by Shade, 2008, p.84).

Some of the key principles in the proposed Charter were the following:

1) privacy is essential to an individual's dignity, integrity, autonomy, well-being and freedom, and to the full and meaningful exercise of human rights and freedoms,
2) there is a legal right to privacy, and
3) an infringement of the right to privacy, to be lawful, must be justifiable.

The draft Charter also proposed that every individual has a right to privacy, including:

1) physical privacy,
2) freedom from surveillance,
3) freedom from monitoring or interception of their private communications, and
4) freedom from the collection, use, and disclosure of their personal information (Shade, 2008).

There were concerns, however, that the bill would cause confusion in terms of the interaction between the right to privacy, the *Criminal Code* and the concept of burden of proof, in addition to other concerns. The situation was aggravated by a delay owing to a federal election and Finestone's subsequent retirement from the Senate. As a consequence, the bill never received the necessary support and was ultimately shelved (Shade, 2008).

On a final note, it is worth pointing out that Canada currently has no legislation specifically aimed at protecting the privacy of youth, although there is a *Canadian Code of Practice for Consumer Protection in Electronic Commerce* (2004), which, while lacking the teeth of legislation, provides some principles and best practices regarding online communication with children and the conduct of e-commerce (Shade, 2008).

Europe

In 1950 the Council of Europe established the Convention for the Protection of Human Rights and Fundamental Freedoms, which declares, "Everyone has the right to respect for his private and family life, his home and his correspondence" (Article 8(1)). In 1983 Germany's Constitutional Court set an important precedent and example when it openly endorsed the concept of "informational self-determination," advocating that "we should be able to control the disclosure and circulation of our own personal information" (Flaherty, 1999, p. 232). More recently, the European Union (EU), similar to Canada, has made significant advances in terms of requiring that personal information not be collected or used for purposes other than those for which is was originally collected, without the consent of the individual concerned. For example, Directive 95/46/EC, introduced by the European Parliament and the Council of the European Union, specifies, "In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to

privacy with respect to the processing of personal data" (1995, Chapter1, Article 1(1)). This protection is defined in the Directive to ensure, inter alia, that any "… processing further to collection shall not be incompatible with the purposes as they were originally specified" and that the personal information in question is appropriately safeguarded. Member states are charged with regulating and enforcing these rights and principles.

In the same year as this Directive was introduced, the EU also put into force the Data Protection Directive (DPD, 1995).

> *"The DPD requires EU member nations to adopt legislation regulating the collection, use, and disclosure of personal information by private organizations and establish Data Protection Authorities to approve, monitor, and assist in enforcing privacy regulation. The DPD has been described as an example of co-regulation, a form of regulation in which the government and industry representatives both participate in the creation and/or enforcement of regulation" (Bushey, 2011, p.11).*

It is also important to note that "all of the European Union countries have the equivalent of privacy commissioners, who are often called data protection commissioners" (Flaherty, 1999, p. 222).

United Kingdom

Further to its obligations as a member of the European Union, the UK is party to various international human rights treaties that recognize the existence of a right to privacy. However, "UK law does not contain a single enshrined right to privacy. No Act of Parliament creates such a right, and the common law only allows a limited recognition of privacy rights in specific situations" (Open University Web site, 2011). As such, there is no legislative provision in the United Kingdom for legal action to be taken on the grounds of invasion of

privacy per se, especially as regards information privacy. There is, however, an Information Commissioner's Office (ICO), which serves as "the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals" (ICO Web site, 2013). The role of the ICO is much like that of the Offices of Canada's Information Commissioner and Privacy Commissioner combined in that, among other responsibilities, it regulates and oversees compliance with certain information legislation[7] and can receive and respond to complaints about organizations' mishandling of personal information.

United States

Individualism in the United States has strongly influenced the discussion of privacy-related policy (Westin, 1967), as it has tended to increase the desire for privacy protection, while decreasing trust in others to respect it, let alone to protect it (Bushey, 2011). Paradoxically, the government is the very entity that has the most power and is best positioned to protect the privacy of individuals from corporations, but precisely because of its size and power, it can also pose the greatest threat to individual privacy (Mendez & Mendez, 2009). This mindset has shaped legislation and its interpretation, as well as the perceived role of government and the development of policy in relation to individual privacy.

Privacy is not assured under the Constitution of the United States, and the U.S has generally favoured arguments for business and government to have unfettered access to personal information for reasons relating to economic growth and national security. However, in 1965 the U.S. Supreme Court explicitly recognized a limited right to privacy that emanated

[7] This legislation includes, the *Data Protection Act*, *Freedom of Information Act*, *Environmental Information Regulations*, and *Privacy and Electronic Communications Regulations*.

from the Constitution. That right was described by one of the justice's as protecting a zone of privacy related to the institution of marriage and intimacy within that relationship, which is consistent with the common perception within American legal circles that the focus of privacy rights is on personal decisions about one's family and private life. But that right has never been clearly defined, and interpretations of the scope of the right have varied considerably depending on the judiciary (DeCew, 2013).

Privacy in the U.S. is regulated under the American *Privacy Act* of 1974 as well as various state laws. The U.S. *Privacy Act* is intended to protect individuals from "an increasingly powerful and potentially intrusive federal government" (Centre for Democracy and Technology, 2013) and applies to all federal agencies. Like Canada's own *Privacy Act*, the U.S. *Privacy Act* allows individuals to access federal government information about them, to correct erroneous information, and to prevent information collected for one purpose from being used for another without consent. The Act also provides instructions for the federal government's proper handling and safeguarding of personal information, and "empowers individuals to control the federal government's collection, use, and dissemination of sensitive personal information" (Centre for Democracy and Technology, 2013). In addition, there is a web of legislation that establishes certain privacy rights and governs an assortment of privacy issues, such as health information (*Health Insurance Portability and Accountability Act* of 1996), school records (*Family Education Rights and Privacy Act* of 1974), driver information (*Driver's Privacy Protection Act* of 1994), video rental information (*Video Privacy Protection Act* of 1988—now virtually obsolete), financial privacy (*Right to Financial Privacy Act* of 1978 and *Gramm-Leach-Bliley Act* of 1999), and so on. More recently, as a response to the increasing threats to the privacy of children and youth posed by advances in data mining

technologies and their intensified application, in 2000 the U.S. *Children's Online Privacy Protection Act* (COPPA) was enacted to better protect children's privacy on the Internet by regulating the collection of personal information from children under the age of 13 and helping to prevent its misuse (Shade, 2008). Among the Act's provisions, COPPA requires parental consent before collecting personal information of children and that parents be given access to, and the ability to correct, all such collected information.

The aforementioned legislation notwithstanding, privacy protection in the U.S. relies heavily on a form of industry self-regulation—the creation and enforcement of privacy rules by industry groups (Hirsch, 2010). The Federal Trade Commission (FTC), which has effectively served as the leading federal agency on the issue of online privacy since about 1997, has initiated a policy of industry self-regulation for Internet privacy and has published guidelines for what it considered to be a comprehensive self-regulatory program. Although the FTC's guidelines place no legal obligations on private sector organizations, the FTC is able to encourage compliance with its guidelines by threatening to seek stronger forms of regulation if the Commission finds that the guidelines are not being followed (Mendez and Mendez, 2009). The core of these guidelines is comprised of the Fair Information Practice Principles (FIPPs), which the Commission adopted from the Department of Health, Education and Welfare's 1973 report entitled *Records, Computers and the Rights of Citizens* (Bushey, 2011).

Australia

Australia has had relatively comprehensive privacy legislation under that country's own *Privacy Act* since 1988. The Act, which applies to most public sector organizations and large corporations, as well as to some smaller businesses, regulates the handling of personal

information about individuals, including its collection, use, storage and disclosure. There is also a provision to allow small private sector organizations not otherwise subject to the Act to "opt-in to being covered by the … Act" (Office of the Australian Information Commissioner Web site, 2013). Under Australia's *Privacy Act*, individuals can file a complaint to the Office of the Australian Information Commissioner, established under separate legislation, for any mishandling of their personal information by organizations bound by the Act.

4.2 Other Responses

Other, non-legislative measures have also been taken to enhance privacy. As an example, Canada's Privacy Commissioner co-founded the Global Privacy Enforcement Network (GPEN) in 2008, which consists of OECD member nations who have agreed to establish an informal network of "Privacy Enforcement Authorities" to foster cross-border cooperation among privacy authorities and which has set out the following tasks for itself:

1) to discuss the practical aspects of privacy law enforcement cooperation,
2) to share best practices in addressing cross-border challenges,
3) to work to develop shared enforcement priorities, and
4) to support joint enforcement initiatives and awareness campaigns (GPEN Web site, 2013).

The Privacy Commissioner has also been an active participant and strong privacy advocate in such international organizations as Asia-Pacific Economic Cooperation, Association francophone des autorités de protection des données personelles, Ibero-American Data Protection Network, the International Standards Organization, and the Organization for Economic Cooperation and Development. Through such forums the Privacy Commissioner has worked to promote information sharing, cooperation among enforcement authorities,

control of cross-border flow of personal information, and the establishment of an international privacy standard (OPC, 2013a).

In terms of technological solutions, strong encryption has become more available to the average Internet user. Anonymizing software and services, which prevent tracking of an individual's Internet activities by concealing any identifying information or linkages, have also become readily available. "Companies offering anonymous Web-browsing and communication services are seeing a huge increase in business since recent news leaks about the U.S. National Security Agency's mass data collection and surveillance activities" (Gross, 2013).

However, while these measures can significantly decrease online risk to privacy, they are not 100 percent effective, and certainly not a panacea for privacy. Concerns have been raised, for example, over demands by some government institutions, particularly in the U.S., requiring that "backdoors" or "Trojan horses" be built into encryption and anonymizing products and services, or that the producers of these products and providers of these services "hand over their encryption keys" so as to enable the government institutions to maintain access as deemed necessary. Also, while these technical solutions offer some added privacy protection, assorted means to overcome them will continue to be sought just as quickly. Moreover, to whatever extent they are effective in helping to secure the confidentiality of certain online activities, such as Web browsing or emailing, and of electronically created and stored documents, they have no effect on the ability of information seekers to monitor and track such activities as Internet purchases by individuals or mobile phone usage, including, who is communicating with whom, when, and from where to where. Finally, they do not prevent legitimate holders of personal information from indiscretions in terms of

indiscriminately sharing their information holdings with others who are not authorized to receive it, nor do they have any impact on visual forms of surveillance.

Another relatively recent development is an increase in the propensity of Web site owners and managers to stipulate exactly what will be done with the information that one provides. This is an important step in the right direction.

4.3 Looking to the Future

Globalization and the rapid evolution of science and technology—especially in the domains of information technology and genetics—combined with changing social and business habits (e.g., the exploding use of social media along with tracking and profiling tools), while offering tremendous opportunities to society, will continue to outpace developments in legislative, policy and ethics frameworks, at least for the foreseeable future. Exacerbated by the increasingly borderless nature of digital information transfer and storage (e.g., the Internet and cloud computing), this scenario will challenge the effectiveness of existing legal frameworks and, consequently, the ability of industrialized societies to protect and promote the privacy interests of individuals. Accordingly, there may be a growing call to broaden the authorities of, and toolsets available to, privacy and information commissioners as well as others mandated to safeguard privacy. There may also be increased calls to intensify collaboration—both domestically and internationally—in such areas as privacy research, monitoring, standards development, and public education on risks and mitigation strategies.

The market for products and services that better protect privacy will also continue to grow, as will demand for privacy to be "built into" all systems vulnerable to privacy

exploitation. In the 1990s, Ontario Information and Privacy Commissioner Dr. Ann Cavoukian developed a set of foundational principles to facilitate personal control over one's information and help protect privacy within the context of information and communications technology. *Privacy by Design* (PbD), as it is known, "is an approach to protecting privacy by embedding it into the design specifications of technologies, business practices, and physical infrastructures," and "is predicated on the idea that … as much as (technology) can be used to chip away at privacy, it can also be enlisted to *protect* privacy. That means building in privacy up front—right into the design specifications and architecture of new systems and processes" (Information and Privacy Commissioner of Ontario (IPC), 2013). PbD advocates a very proactive, vice reactive, approach to anticipating and preventing privacy-invasive events and seeks to ensure that personal information is automatically protected in any given information system or business practice by default. "This … solution has gained widespread international recognition, and was recently recognized as a new global privacy standard" (IPC, 2013). This approach is similar in concept to the notion of "security by design," which, it is commonly believed, if it were incorporated into the original design of the Internet, would have pre-empted many of today's online security concerns.

5. *Arguing the Ethical Imperative*

Having demonstrated the relevance of privacy on both individual and societal levels, there remains the need to demonstrate the second part of the hypothesis—that the preservation and restoration of privacy constitutes an ethical imperative. To this end, in the following sections I argue the case from four distinct ethical perspectives—utilitarian, as put forward by John Stuart Mill; monistic deontological, as advocated by Immanuel Kant; social contract, as argued by John Rawls; and ethical rationalist, as proposed by Alan Gewirth. It is worth noting that all four perspectives have relevance not only to the issue of privacy in general, but specifically to *information* privacy, as well, despite that two of the four philosophers—Kant and Mill—lived well before the advent of either the Information Era or the Internet.

5.1 Utilitarian and Liberalism-oriented Perspectives of John Stuart Mill (1808-1873)

In this section I address the issue of privacy from the perspective of John Stuart Mill's version of *ideal* and *eudaemonistic*[8] rules-based utilitarianism and political liberalism. Mill was a strong advocate of the concept of rules or principles that, when applied, would offer the best long-term prospects for human happiness and well-being. I thus begin by setting out the relevant principles of Mill's utilitarian moral doctrine and liberalism-based political theories and then examine various types of privacy incursions through the lenses of these principles. In so doing, I present the case for the second element of my hypothesis, i.e., that the preservation and restoration of privacy constitutes an ethical imperative.

[8] Classic eudaemonistic utilitarianism defines moral good in terms of the happiness that an action produces or is capable of producing.

The arguments presented here are based on the following principles set out, or at least strongly endorsed, by Mill:

1) ***Greatest happiness principle (GHP)***: Happiness, pleasure and human well-being, along with avoidance of pain, harm and suffering (hedonic calculus) are what matters ultimately—what is right is what ultimately generates more happiness. This principle is also referred to as the "ultimate standard," "the first principle," "the ultimate source of moral obligations," and "the fundamental principle of morality" (Mill, 1871, chap. 2).
2) ***Consequences***, ***outcomes*** or ***results***: The concept of *outcomes* is central to the GHP and the utilitarian philosophy. Outcomes (or results or consequences) serve as the ultimate measuring stick of morality (Mill, 1871).
3) ***Intention***: "The morality of an action depends entirely on the intention—that is, upon what the agent wills to do" (Mill, 1871, chap. 2).
4) ***Veracity***: According to Mill, "… deviation from truth (weakens) the trustworthiness of human assertion which is not only the principle support of all present social well-being, but the insufficiency of which does more than any one thing that can be named to keep back civilization, virtue, everything on which human happiness on the largest scale depends" (1871, chap. 2). Mill refers to veracity as "sacred," although he acknowledges the need for "possible exceptions" and some "latitude" in any ethical creed to accommodate very special circumstances, such as where there may be conflicting obligations; however, "in order that the exception may not extend itself beyond the need, and may have the least possible effect in weakening reliance on veracity, it ought to be recognized, and, if possible, its limits defined" (1871, chap. 2).

5) ***Virtue***: Mill asserts that "the multiplication of happiness is, according to the utilitarian ethics, the object of virtue" and that virtue is one of the precursors of happiness (1871, chap. 2).

6) ***Rights*** and ***duty*** (particularly, basic liberal *rights*, i.e., consistent with those generally conferred by a liberal democracy and with the other principles and values set out herein, and the *duty* to promote good consequences and happiness): According to Mill, the GHP, as the first principle, can be invoked to arbitrate between conflicting "rights and duties," on the one hand, and "subordinate principles" (also referred to as "*secondary* principles"), on the other (1871, chap. 2). Mill also asserts, "It is the business of ethics to tell what are our duties, or by what test we may know them" (1871, chap. 2). Mill acknowledges, however, that duty is not the sole legitimate motive—the vast majority of our actions are generated by other motives, "and rightly so done, if the rule of duty does not condemn them" (1871, chap.2).

7) ***Justice***: Mill places a heavy emphasis on justice, particularly in the sense of "fairness" (Mill, 1869a,1869b, 1871; Bercer, 1979).

8) ***Respect for human dignity***: For Mill the concept of dignity encompasses, inter alia, self-respect, self-esteem and the esteem of others (1869a, 1869b, 1871).

9) ***Self-protection / self-defence***: Mill claims that "the sole end for which mankind are warranted, individually or collectively, in interfering with the liberty of action of any of their number, is self-protection" (1869a, chap. 1). He also acknowledges, "It is natural to resent, and to repel or retaliate, any harm done or attempted against ourselves, or against those with whom we sympathise," and associates the latter with morality (1871, chap. 5).

In addition, Mill makes reference to an individual's "instinct ... of self-defence" and to "the acknowledged justice of self-defence" (1871, chap. 5).

10) ***Social utility*** (i.e., conforming to the general good, as perceived by Mill, and to the common interests of society and its members): Mill insists that, in settling matters involving irreconcilable principles of justice, "Social utility alone can decide the preference" (1871, chap. 5). He also argues that moral requirements that "stand higher in the scale of social utility ... are therefore of more paramount obligation, than any others" (Mill, 1871, chap. 5).

11) ***Impartiality*** and ***the golden rule***: Impartiality regarding the distribution of happiness is fundamental to utilitarianism; so, according to Mill, is *the golden rule*—"To do as you would be done by, and to love your neighbour as yourself, constitute the ideal perfection of utilitarian morality" (1871, chap. 2).

12) ***Respect for autonomy***, ***self-determination*** *and* ***non-interference***: Individual autonomy is fundamental to Mill's version of utilitarian liberalism and self-determination, and non-interference can be viewed as an extension of autonomy. Additionally, Mill is clear that only under very specific circumstances can an individual or a collective interfere with the "liberty of action" of another (1869a, chap. 1).

13) ***No-harm / prevention of harm***: Mill advocates the avoidance of harm and suffering, such as is caused by murder, theft, poverty and disease, as well as by "the unkindness, worthlessness, or premature loss of objects of affection (and other) positive evils of life" (1871, chap. 2).

14) ***Representative democracy*** and ***good governance***: In Mill's view, a legitimate government is responsible to, and must represent the interests of, its constituents, including conferring

upon them, and protecting, basic individual rights and civil liberties (consistent with the fundamental principles of utilitarianism and liberal democracy). It must also fulfil its responsibilities competently (1862, 1869a).

15) ***Freedom of speech/expression***, ***association***, ***worship*** and ***occupation***: Mill is a strong proponent of these freedoms for everyone (Mill, 1869a).

Illicit access to, use of, or sharing of personal information contravenes Mill's principle of *respect for human dignity* [9] as it fails to actively recognize and respect an individual's potential sensitivity regarding that information or desire not to have it used in a particular manner or made available to someone who has not been authorized to have it. Fried's (1975) claim that privacy threats pose a threat to our very integrity as persons, combined with Hosein's claim that privacy is a prerequisite for human dignity (Hosein, cited by Shade 2008), Bloustein's (1964) argument that surveillance and privacy invasion constitute an affront to human dignity, and the 1980 Williams Commission Report, which links privacy to the preservation of human dignity and to personal freedom (cited by Lawson & O'Donoghue, 2009), highlights the importance of respect for privacy and its protection, particularly in terms of compliance with Mill's principle of respect for human dignity.

Wrongful access to, or treatment of, personal information also fails to comply with the principles of *impartiality* and *the golden rule* because, in most instances, the action taken with respect to the personal information is not consistent with the manner in which the actor would like his *own* personal information to be treated. Moreover, the unauthorized monitoring and indiscreet sharing of personal information limits one's sense of freedom of expression and

[9] The first occurrence of each Millian principle is italicized.

communication, which directly violates Mill's principle of *freedom of speech/expression* and indirectly contradicts his principles of *autonomy* and *self-determination* because, as Gus Hosein argues, privacy provides a form of core protection for individual autonomy (Shade, 2008), and its degradation has the effect of inhibiting one's openness to self-expression and self-actualization, thereby impeding autonomy and self-determination. In addition, any negative *consequences* resulting from unauthorized disclosures of personal information or other forms of privacy invasion would presumably be inconsistent with any outcome intended by the person whose privacy was invaded and, hence, autonomy and self-determination as well as *happiness (GHP)*, certainly on the part of the victim(s), would be negatively impacted. A harmful outcome would also contravene Mill's *no-harm* principle.

If, as it has been suggested, privacy is essential in order for one "to choose and realize one's place in society" (McFarland, 2012, p. 2), and if it has instrumental value in the development and management of social relationships, then it has *social utility*. Similarly, if, as Fried (1970) argues, trust, friendship and love are possible only if persons enjoy mutual privacy, and if, as Inness (1992) contends, privacy allows one to fulfill one's needs of loving and caring for others, then again social utility is surely served by privacy. Thus, should privacy invasion continue to escalate, there will be a corresponding *decrease* in any social utility that might have been initially perceived in society's allowing such degradation of privacy to occur in the first place, especially if, as can reasonably be expected based on current trends, public distress intensifies accordingly. Moreover, consequences like embarrassment, social ostracism or other forms of discrimination, resulting from unauthorized disclosure of sensitive personal information, such as medical or law enforcement-related

records, for example, are contrary not only to Mill's principle of social utility, but also to his principles of *justice*, in the sense of fairness, and the GHP.

Where non-consensual disclosure of personal emails, Web sites visited or other personal information leads to the inhibition of political, religious or other personal views or affiliations, then Mill's principles of autonomy and self-determination, as well as *freedom of speech, association* and *worship*, are all infringed, as are basic liberal democratic *rights*. The principle of social utility is also breached, given that the inhibition of free speech and communication stifles creativity and is both antisocial and counter-productive and, hence, contrary to the interest of society writ large.

In instances where the reckless public disclosure of incomplete, misleading, misrepresentative or incorrect personal information proves inadvertently harmful, Mill's principles of justice, *veracity*, *duty*, respect for human dignity and social utility are all compromised. But what if the disclosed personal information is *intentionally* misleading or misused—and in the present day context such occurrences are not particularly remote—such as in the theft of passwords or identity, and the results are clearly harmful, as might be the case where the theft and subsequent actions establish precursors that ultimately lead to such ills as fraud, financial theft, reputational damage, blackmail, embezzlement, harassment, or even physical harm? In any such scenario the information disclosure and/or abuse would constitute gross privacy violation and would contradict a number of Mill's utilitarian principles, including no-harm, justice, respect for human dignity, *virtue* and the golden rule, further to social utility. Moreover, given the absence of honesty in such actions and their impact on one's trust in others and on the trustworthiness of the perpetrators, Mill's principle of veracity would condemn them. In addition, autonomy and self-determination would be

impacted, as might *freedom of occupation* (particularly in the case of reputational damage), and Mill's principle of *non-interference* would clearly be breached. Finally, it is difficult to imagine a scenario here that would uphold the GHP, short of, perhaps, one where the loss of privacy of a highly wealthy tyrannical family were to lead to the theft and redistribution of that family's excess wealth to a large population of needy individuals, or something along that line of thought. Even in that instance, however, numerous other principles (e.g., veracity, virtue, rights, respect for human dignity, impartiality and the golden rule, respect for autonomy, self-determination and non-interference, no-harm) would come into play that would more than offset any potential justification on purely GHP grounds.

On matters of national security and law enforcement, Mill would find it quite understandable and even appropriate for state authorities to monitor the activities of select citizens where they are reasonably deemed to constitute a potential threat to the security of the state and/or safety of its (other) citizens. Such monitoring, i.e., incursion on individual privacy, would be justified in his view based on the principles of *self-protection*, prevention of harm, duty (i.e., of the state to protect its citizens and to maintain law and order), social utility and, ultimately, the GHP. However, Mill would have serious ethical reservations if and where the democratic rights of the individuals concerned, or their dignity, are not respected. In a more extreme case, such as the highly publicized one involving Maher Arar, where an individual is apprehended, confined, deported and interrogated, and where the grounds for suspicion are, in part, related to the individual's religious affiliations, then the precursory surveillance—i.e., temporary partial suspension of privacy—and subsequent apprehension indirectly violates freedom of association and worship, as well as one's fundamental rights as a citizen of a democratic state. In addition, where his treatment while in detainment includes

torture, as an ultimate consequence of the privacy invasion, then that privacy breech (as well as the ensuing actions) violates Mill's principle of respect for human dignity. Similarly, where the accuracy or analysis of any given personal information proves to be flawed and leads to unjust consequences for the person or persons under scrutiny, Mill would find such treatment of personal information to be reckless, at best, and certainly in contravention of the principles of justice (as fairness), veracity, virtue and the GHP.

In instances where surveillance is used as an instrument of control or oppression, Mill would find such action contrary to the principles of autonomy and self-determination at the individual level, given that, as Bloustein (1964) notes, surveillance and invasion of privacy in general reduces self-determination. Instances of oppression, in particular, also contravene the principles of justice and respect for human dignity. The one possible exception to the utilitarian disapproval of privacy invasion for purposes of control—but never oppression—might be in instances where a compelling social utility argument can be made, such as in the event of a specific national crisis. But even in such an instance the action taken would need to be the minimum necessary and to be of very limited duration, bearing in mind that when there is a conflict between *act*-based utilitarianism, such as would be the case in committing privacy violations for immediate or short-term social utility purposes, and *rules*-based or principle-based utilitarianism, Mill's doctrine ultimately favours the latter.

Viewing the issue of privacy through the lens of fundamental democratic rights and freedoms, which are two priorities of Mill's political theory, I point first to Uteck's (2009) claim that privacy invasion impairs aspects of individuality that ought to be protected in a free and democratic state, and, second, to Chandler's (2009) argument that complete openness to public scrutiny (owing to privacy invasion) will diminish not only dignity, autonomy and

individuality, but also liberty. It is important also to highlight the loss of freedom—i.e., freedom to be oneself—that results, as McFarland (2012) points out, from excessive public visibility. Mill would certainly heed these arguments, as he would Johnson's (2009) claim that privacy is a social good that is essential for democracy, Steeves's argument that privacy is essential to the democratic process (Shade, 2008), and Allen's (1988) assertion that a lack of privacy opens the domestic sphere to intrusion by the state, the latter being incompatible with the principles of autonomy, self-determination and non-interference, as well as democracy and democratic rights. Mill would be captivated by these arguments because they ascribe great importance to privacy based on Mill's own politico-ethical principles.

However, Mill would also support Westin's (1967) observation that liberal democracies require a proper balance between privacy, on the one hand, and disclosure and surveillance, on the other, in order to protect democratic processes. By extension, he would also endorse McFarland's (2012) argument that privacy cannot be absolute and that governments require certain personal information to function effectively, to provide for the security of the state and its citizens, and to distribute benefits and obligations equitably, as this would be consistent with his principles of self-protection (at both state and individual levels), GHP, duties (in respect of the common good), social utility, justice (as fairness), and democracy and *good governance*. This perspective would also be consistent with Mill's principle of self-protection—in this instance the self-protection of society or of the state, rather than of the individual—and with his contention that "the only purpose for which power can be rightfully exercised over any member of a civilized community, against his will, is to prevent harm to others" (Mill, 1869a, chap. 1).

On a final note, since Mill values veracity and trustworthiness, as well as virtue, one can reasonably conclude that Mill would call for openness, honesty and trustworthiness, as well as virtuous behavior in general, from those who would be in a privileged position to impact privacy, including to use and abuse personal information, in particular, and to exploit privacy, more broadly. Similarly, it is reasonable to deduce that Mill would also value *trust* itself, because without it, veracity and trustworthiness have no utility. To cite a workplace or employer-employee scenario—which is especially apropos, given that an employer's focus is typically on a type of outcome, best known as the "bottom line"—excessive monitoring of employees, which constitutes a form of privacy incursion, indicates a lack of trust and thereby contravenes that value and Mill's ethics; it also negatively impacts employee emotional well-being and happiness, contrary to the GHP and, again, Mill's ethics. A counter-argument can be made, however, that, to the extent that such monitoring is effective in reducing risk to the employer and increasing productivity, and to the extent that this benefits not only the employer but also the workforce, such as through increased remuneration and/or job security, then the monitoring might be deemed to benefit virtually all concerned. In such a case the guidance offered by the GHP becomes less clear, as it is dependent on the net impact on happiness—in this instance the difference between declined morale and happiness resulting from monitoring and privacy invasion, on the one hand, and possible increased happiness resulting from improved remuneration and/or job security, owing to greater corporate success (though possibly short-lived), on the other.

The foregoing indicates that the concept of privacy is strongly supported by—even inextricably linked to—Mill's utilitarian ethics and liberalism-based politico-philosophical convictions.

5.2 Monistic Deontological Perspective of Immanuel Kant (1724-1804)

In this section I examine the issue of privacy through the eyes of Immanuel Kant and the lens of his monistic deontological ethical and philosophical doctrine. Specifically, in my analysis I apply the following Kantian principles:

1) ***Categorical imperative*** (both variants or formulations): ***Respect for persons and human dignity*** (also known as the *practical imperative* or *formula of humanity as an end in itself*) advocates that one should "act that you use humanity, in your own person as well as in the person of any other, always at the same time as an end, never merely as a means" (Kant, 1785/2012, p. 41), based on the contention that humans are the only rational beings and moral agents, and that, unlike all other beings and objects, who have only instrumental value, humans have unconditional, intrinsic value and must, therefore, be treated with respect and dignity, regardless of circumstance. ***Universalizability*** (also known as the *formula of universal law* or the *universal imperative of duty*) is the other variant of the *categorical imperative*, which espouses that one should "act only according to that maxim through which you can at the same time will that it become a universal law" (Kant, 1785/2012, p. 34).
2) ***Intention***: The intention behind an action, irrespective of the consequence or outcome of that action, is what Kant considers to be of particular moral significance—virtue is found in the good will or good intention of an agent (Guyer, 1998).
3) ***Duty***: "To be beneficent where one can is one's duty" (Kant, 1785/2012, p. 13). According to Kant, good will or good intention is manifested in the performance of an action for the purpose of fulfilling duty (Guyer, 1998). When performing an action

"without any inclination, solely from duty," then, and only then, "does it have its genuine moral worth" (Kant, 1785/2012, p. 14).

4) ***Rights*** (including individual rights and human rights): A strong advocate for human rights, Kant contends that, "Human rights must be kept whole, no matter what that may cost the powers that be. … all politics must bend its knee before human rights" (Kant, cited in Horton, 2007).
5) ***Autonomy*** and ***freedom of action*** (of the individual): "Autonomy is … the ground of the dignity of a human and of every rational nature" (Kant, 1785/2012, p. 48). Kant submits that human autonomy is both the supreme value and the limiting condition of all other values (Guyer, 1998). In espousing autonomy and freedom of action, Kant presupposes conformity with the categorical imperative as well as independence from any incentives or interests (Kant, 1785/2012).

It is worth noting that Kant considers his principles to be essentially irrefutable in the sense that all rational agents would agree to them, certainly under idealized conditions (Ashford & Mulgan, 2012). As well, in setting out his philosophical doctrine, Kant is not deterred by, or even particularly interested in, concrete, pragmatic concerns or practicalities such as one normally faces in daily life. Consequently, some might view his doctrine as unrealistic or impracticable; others, however, might find it refreshingly pure, unobstructed and representative of the loftiest ideals of human existence.

Recalling the reported impacts on autonomy of even the *threat* of privacy incursions, Kant and his followers would have significant unease with the privacy impacts of the integrated digital environment and the manner in which it has been managed—or not managed—based on the principles of *autonomy* and *freedom of action* of the individual. The

concerns would be compounded when also taking into consideration Kant's *practical imperative*, wherein the end does not necessarily justify the means, because privacy invasion contravenes this principle where the sole *intention* is to exploit others exclusively for personal gain or out of other purely selfish motives, and not necessarily to offer any benefit to the affected user, for example through improved service or products, let alone to accommodate their express wishes—which the principles of respect for persons (practical imperative) and autonomy ultimately call for. The rationale for this claim is that such behavior treats others—in this instance the targeted or victimized user—merely as means to an end, rather than as ends in themselves, and in so doing ascribes to others only instrumental value, rather than intrinsic value. As McFarland (2012) notes, based on Kant's doctrine, "Reverence for the human person as an end in itself and as an autonomous being requires respect for personal privacy" (2012, p. 1). Also, as Deborah Johnson has observed, "To recognize an individual as an autonomous being, an end in himself, entails letting that individual live his life as he chooses. Of course, there are limits to this, but … when one cannot control who has information about one, one loses considerable autonomy" (Johnson, cited in McFarland, 2012, p. 2). Further elaborating on this theme, McFarland argues, "Autonomy is part of the broader issue of human dignity, that is, the obligation to treat people not merely as means, to be bought and sold and used, but as valuable and worthy of respect in themselves. … personal information is an extension of the person. To have access to that information is to have access to the person in a particularly intimate way" (2012, p. 3). Hence, mistreating personal information translates to mistreating the person concerned and disregarding their dignity. I would further argue that deliberately concealing or obfuscating the intended treatment of a user's personal information, as occurs in the absence of full disclosure when collecting

personal information, again violates Kant's practical imperative, as it, again, treats persons as means rather than ends.

Privacy invasion also raises the matter of consent. Kant submits that an action affecting another person that is taken without regard to the latter's consent is disrespectful of that person and of human dignity because treating humanity as an end in itself requires, at the very least, the possibility of rational consent from a party affected by one's actions (Guyer, 1998). Such an action also detracts from that individual's autonomy. Thus, failure to seek consent to a given privacy incursion once again defies Kant's practical imperative as well as his principle of autonomy. McFarland suggests that privacy invasion also dehumanizes its victims by commodifying them. He reasons, "When some personal information is taken and sold or distributed, especially against the person's will … it is as if some part of the person has been alienated and turned into a commodity. In that way the person is treated merely as a thing, a means to be used for some other end" (McFarland, 2012, p. 3). This is yet another argument endorsing respect for privacy based on Kant's practical imperative.

Kant would also argue that accessing an individual's personal information without consent is not respectful of that individual as a free and rational being because it disregards that person's choice to protect, or at least not to disclose, that information, and it treats the person as an object instead of a rational agent. As well, it impinges on, and disrespects, one's freedom to define oneself and one's relationships with others. Moreover, unauthorized surveillance and the nonconsensual collection, sharing or careless handling of personal information defies respect for persons and for human rights as well as for freedom of action on the grounds that it interferes with the choice of an individual, as a rational chooser, to act independently of external observation and scrutiny (Benn, 1978). Kant would also maintain,

however, that while privacy is essential for freedom of action, as a citizen of a liberal state one must accept certain limits on that privacy and freedom of action that take into account the rights of others (Benn, 1971).

To consider another principle, Kant also attaches great importance to the notion of *duty*, which, when taking into account Kant's social contract views and clear endorsement of the power and integrity of the state (Rauscher, 2007), makes it reasonable to surmise that Kant would support the stance that governments have a duty to protect and promote the safety and well-being of their citizens. He would likely also acknowledge, therefore, that governments have a duty to protect the *privacy* of their citizens, recognizing the inextricable and well-established link between privacy, on the one hand, and safety and well-being, on the other.

Kant would also contend that there is a duty on the part of everyone who is in a position to impact privacy not only to refrain from taking advantage of that position and deliberately exploiting privacy, but also to take measures to avert privacy violations by others. Kant enumerates four distinct categories of duties. One of these, referred to as *perfect duties to others*, consists of both proscriptions and prescriptions of certain kinds of actions in relation to other persons that, when committed, in the first instance, or avoided, in the second instance, constitute immorality on the part of the actor (Guyer, 1998). Deceitful or negligent behaviour, particularly where it causes defamation of, or injury to, someone is included among such proscribed actions. Also included are behaviours that ultimately impinge on another's autonomy or freedom of action, as Kant asserts that perfect duties to others include both the prohibition of injury to the dignity of others as free agents and the prescription of efforts to improve the conditions for others to exercise their own freedom (Guyer, 1998). Thus, when personal information is collected, managed, stored, used or shared in a manner

that would not be condoned by the source of that information if the source were fully informed of the true intentions and associated risks, then it violates Kant's principle of perfect duties to others by virtue of its deceitfulness and negligence, as well as its impact on autonomy, freedom of action, and dignity.

Kant further distinguishes between two types of duties: *duties of justice* and *duties of virtue*. The former consists of those duties that can appropriately be enforced through public, juridical compulsion and where such force is both necessary and able to preserve freedom; the remainder of duties, which are suitable for moral assessment but not for coercion, are duties of virtue (Guyer, 1998). It can be argued that privacy invasion, in most of its forms, falls within one or both categories of duties, and that the concept of duties of *justice* calls for legislative and policy solutions to protect privacy, where feasible, and the concept of duties of *virtue* places on anyone who is in a position either to violate or to protect privacy a moral obligation to act in accordance with the remaining ethical principles laid out by Kant.

From the perspective of *universalizability*, the other variant of the *categorical imperative*, a person's action can be considered universalizable if, and only if, that person is comfortable with any and all other persons or entities performing the same action or engaging in the same activity. If asked whether it is desirable for *all* persons, corporations or even governments to seek out, use and share, either inadvertently, due to poor information management practices, or deliberately, personal information without the explicit consent or even knowledge of the individual concerned—i.e., to violate their privacy—most persons, including those contemplating such actions, would agree that it is not. Hence, Kant would condemn privacy invasion on the grounds that his principle of universalizability would not support it.

The Facebook Beacon fiasco previously mentioned (pp. 23-24) is a stellar example of behavior that is disrespectful of individual privacy and would clearly be counter to Kant's doctrine—perhaps most notably the categorical imperative and duties of virtue. The Google Buzz event was perhaps slightly less disrespectful, in comparison with the Facebook Beacon one, but only because subscribers to Google's "Gmail" service were notified when logging in to their email accounts; however, it nevertheless failed to respect the privacy wishes of the vast majority of users and offered users the option to opt out only *after* their privacy had already been violated, instead of making the opt-out option the default position and leaving it to the user to elect to opt in, with full awareness of the risks, should they so choose. Hence, the Google Buzz example, like the Facebook Beacon one, also illustrates behaviour that clearly contravenes Kant's doctrine.

Finally, in considering the morality of an act, such as privacy invasion, Kant would consider the intention behind it. Where the sole intention of a given privacy infringement is to address legitimate national security concerns, for example, then, consistent with the duty of the state to maintain its integrity and the safety of its citizens, and provided that the action 1) is the minimum necessary to fulfill that objective, 2) is consistent with the actor's other duties and obligations, and 3) does not unduly infringe on any individual rights, including autonomy, Kant's doctrine can condone it. In most circumstances, however, privacy encroachment cannot be condoned based on Kant's intention principle.

In summary, based on the principles laid out herein, Kant's deontological moral doctrine speaks strongly against privacy infringement in general, and can condone it only under very limited circumstances and with certain caveats. Specifically, anyone in a position to infringe privacy has the duty to ensure that any infringement undertaken is carried out with

the utmost vigilance and respect for those whose privacy is being compromised, including, wherever possible, obtaining their explicit, informed consent to forego some degree of privacy, normally in return for a perceived benefit that clearly outweighs the ill of the privacy curtailment, or, where consent is not possible or practicable, as is often the case in regard to national security or law enforcement, for example, ascertaining that the infringement is justified by a duty, principle or greater good that undeniably surpasses the moral obligation to respect and uphold privacy.

5.3 Perspective of Social Contract Theory as Presented by John Rawls (1921-2002)

John Rawls is arguably one of the most influential recent social contract theorists. Like Kant, Rawls seeks principles to which every rational person ought to agree and advocates a form of universalizability in his approach. However, he takes this approach a step further. To ensure impartiality in setting out a fair and just societal constitution, Rawls proposes visualizing a hypothetical "veil of ignorance" scenario, wherein those in a position to create the ethical framework for a virtual society, in which they themselves would live, have no idea of what their particular circumstances—ethnicity, sex, appearance, health status, social class, talents, abilities, religious beliefs or conception of the good life—or societal role would be. Rawls puts forth that the expulsion of any such information that could bias one's perspective essentially forces one, even if highly selfish, to adopt an ethical outlook, and that any principles emerging from that exercise would be fair because each person would know that they could end up being anyone and would, therefore, have concern for all (Ashford & Mulgan, 2012). Rawls further suggests that participants in this "original position" would tend toward a low-risk strategy whereby they would be guaranteed the highest minimum levels of

freedom, opportunity and wealth, even if it resulted in lower average levels for the population overall. Rawls suggests that in this scenario people would tend toward being governed by the two following principles of justice: first, that each person is given the right to the greatest degree of fundamental liberty compatible with the same for others (***equal liberties principle***); and, second, that social and economic inequalities are to be adjusted so as to advantage those who are the worst off (***difference principle***; Rawls, 1971).

In his book *A Theory of Justice*, Rawls (1971) sets out a list of what he calls "natural duties." Included in the list are the following:

1) the ***duty not to injure***, not to harm the innocent, and not to be cruel;
2) the ***duty to help one another***;
3) the ***duty of justice and fairness*** (including, to be just, to promote justice, and to support and comply with institutions that are just); and
4) the ***duty of mutual respect***.

These *natural duties* exist irrespective of circumstance and of any action taken on the part of any individual. Rawls also acknowledges the existence of inherent *obligations*, which arise out of an individual's voluntary actions, such that she has, in some manner, taken them on through participation in some activity or process. According to Rawls,

> *"The content of obligations is always defined by an institution or practice the rules of which specify what it is that one is required to do. And … obligations are normally owed to definite individuals, namely, those who are cooperating together to maintain the arrangement in question" (1971, p. 113).*

Moreover, obligations can be incurred when "… one has voluntarily accepted the benefits of the arrangement or taken advantage of the opportunities it offers to further one's interests" (1971, p. 112).

It is the sum of natural duties and obligations that, according to Rawls, forms one's set of ethical *requirements*, i.e., the moral rules that govern an individual's conduct. These requirements include, inter alia, the concept of consent. They also comprise a subset of Rawls's broader social contract theory, according to which for an agreement to be binding the signatories must all enjoy a reasonably fair bargaining position and any "conditions must be defined so as to preserve the equal liberty of the parties and to make the practice a rational means whereby men can enter into and stabilize cooperative agreements for mutual advantage" (1971, p. 345). Rawls does not see the agreement as binding on an individual in instances where "pertinent information was deceitfully withheld from him" (1971, p. 345), or, in cases where there is a vendor-consumer or marketer-consumer relationship, if the nature of the product or service is not fully disclosed.

In his more recent writings, Rawls explicitly endorses the principles of ***autonomy***, ***liberty*** and ***free choice***, as well as ***reciprocity*** (Christman, 2009). He also places individual rights ahead of the common good, even ahead of any claim based on the good that would result to the individual (or to others) whose rights were violated (Rogers, 2002). In fact, Rawls emphatically avows the supremacy, even absoluteness, of justice and individual rights and liberties when he states,

> *"Each person possesses an inviolability founded on justice that even the welfare of society as a whole cannot override. For this reason justice denies that the loss of freedom for some is made right by a greater good shared by others. It does not allow that the*

sacrifices imposed on a few are outweighed by the larger sum of advantages enjoyed by many. Therefore in a just society the liberties of equal citizenship are taken as settled; the rights secured by justice are not subject to political bargaining or to the calculus of social interests" (Rawls, 1971, pp. 3-4).

With specific regard to privacy, therefore, whatever benefit might be perceived to come from a given privacy incursion, or from a lack of commitment to prevent it, whether that benefit is commercial or instrumental to meeting some governmental or personal objective, Rawls would condemn it on the grounds that the resultant loss of freedom and infringement of rights of those whose privacy is impaired would morally outweigh the perceived benefit, however much greater that perceived benefit might be.

As discussed earlier, and without restating much of what has already been expressed in previous sections, the collection, use and distribution of personal information without authorization reduces a person's control over their own destiny and therefore infringes the exercise of their autonomy, liberty and freedom to choose—three important principles in Rawls's doctrine. It is also disrespectful, injurious, and inconsistent with the duty to help one another, as advocated by Rawls. In addition, it fails the tests of justice, fairness and consent, further principles of Rawlsian ethics and philosophy. Moreover, those whose personal information is being exploited are normally not in a position to reciprocate; hence, such activity also defies Rawls's ethical requirement for reciprocity. Lastly, privacy invasion violates the moral obligations set out by Rawls for full and honest disclosure and, in most instances, for mutual advantage.

Rawls would argue that both the obligations incurred by an information seeker when he initially engages in an endeavour that precipitates an interest in someone's personal

information, and the implicit contract that he enters into when the person whose personal information he is seeking participates in an activity that renders her vulnerable to a privacy concession are violated in any attempted privacy infringement because of the asymmetrical nature of the relationship. For example, in a case where someone exploits information systems and networks, or any technology, for that matter, for the purpose of personally benefiting from covert or manipulative access to personal information, the agent is highly likely to be in a position of greater awareness of the situation than any person whose privacy is being compromised and, therefore, to be party to a significant inequality. The significant advantage, in terms of knowledge, expertise and power, held by the information seeker over the information target, owing to the former's position and/or awareness of the situation, precludes the parties from enjoying a fair bargaining position. In addition, the actor's obligation to disclose all pertinent information in advance is not met. Ergo, based on Rawls's social and ethical doctrine, the information seeker lacks both contractual and moral grounds on which to justify his actions. What is more, extrapolating from Rawls's second principle of justice, which in this context could be interpreted to state that an inequality of one social group or member thereof relative to another must be adjusted so as to advantage the worse off, and applying this principle to the present scenario, the entity seeking the information is obliged to ensure that whatever action he undertakes in relation to the person whose personal information he is seeking—in this instance the entity who is clearly the worse off—advantages the latter so as to diminish or eliminate altogether the inequality. Given the improbability of this occurring, such privacy invasion would generally qualify as immoral, based on Rawls's difference principle and social contract theory.

In conclusion, Rawls's insistence on the absolute inviolability of persons "founded on justice" and his contention that the loss of freedom for some cannot be made right by a greater good shared by others essentially renders moot—with only one exception—any argument that might be put forth in attempting to justify or rationalize a societal tolerance of privacy infringement on the basis of some greater good that it yields or facilitates—such as commercial expediency, economic growth, state security, or law enforcement—given that privacy infringement has been shown to defy fairness and justice and to limit freedom. The one exception, I would submit, might be an instance where it could be unequivocally shown that deference to one's privacy would ultimately lead to an infringement of even greater magnitude on the liberty and rights of another individual or group of individuals. As Garrett (2002) submits, in extrapolating from Rawls's equal liberties principle, privacy enables us to pursue our personal conceptions of the good with those with whom we wish to associate, provided that, in so doing, we do not violate the rights and liberties of others.

5.4 Ethical Rationalist Perspective of Alan Gewirth (1912-2004)

Alan Gewirth (1987) speaks of the need to include economic and social rights—e.g., housing, employment, food, education, social security, health care, unemployment compensation—under the rubric of human rights, along with political and civil rights—e.g., voting, participating in government, equal protection of the law, freedom from arbitrary arrest or detention, freedom of movement and association, freedom of religion—and points to this recognition by the Universal Declaration of Human Rights, 1948. He also places *human* rights within the ambit of *moral* rights and argues for the "justificatory primacy of morality," claiming that legal rights must derive from, or at least be consistent with, human rights and,

hence, overarching moral rights, otherwise the legal rights have no legitimate foundation and are of questionable validity (Gewirth, 1987, p. 239).

Gewirth also claims that, given that all moral precepts contend with how persons ought to act, "the most central precepts of morality deal with the abilities and conditions that must be fulfilled if persons are to be able to act either at all or with general chances of success in achieving the purposes for which they act" (1987, p. 241). Gewirth suggests that there are two such necessary conditions and generic features, namely freedom and well-being. He further asserts that *freedom* consists of two components—i.e., unforced choice and knowledge of relevant circumstances—while *well-being* includes a variety of components that "fall into a hierarchy of goods, ranging from life and physical integrity to self-esteem and education" (Gewirth, 1987, p. 241). Gewirth is clear on the incontrovertible application and distribution of the aforementioned conditions, namely that "all humans should equally have freedom and well-being … and … they should have them as *rights* … something to which they are entitled" (1987, p. 241), and that "other persons ought … not to interfere with their having freedom and well-being." He adds that these "rights" constitute both "human rights" and "generic rights," given their universality and generic application.

Based on the above, in instances where the conditions necessary for a person to be able to achieve the objective(s) of his or her actions are deliberately corrupted by an external actor, then the latter's actions become subject to moral scrutiny. In reference to privacy in particular, violations of an individual's information privacy impair, in no small way, personal *choice*—a component of freedom, which, in turn, is the first of Gewirth's two necessary conditions—in terms of the ability to choose what personal information one discloses to whom, when, how and under what conditions or with what caveats. Such violations also limit

one's freedom to realize personal objectives by impairing one's abilities to control personal information, to conduct business and pursue personal interests using information technology without external interference or awareness, or without even the *fear* of external interference or awareness, to communicate freely and privately with others and to define one's relations with others, and to otherwise act with autonomy, self-determination and a view to self-actualization.

On examination of the issue of information privacy with reference to the second component of freedom, i.e., *knowledge of relevant circumstances*, it becomes clear that this condition is not satisfied in the case of surveillance or privacy invasion of any type where the person targeted is unaware of the action being taken in regard to him and, hence, has limited knowledge, at best, of the "relevant circumstances" under which he is operating. Once again, therefore, those conducting the surveillance or otherwise encroaching on another's privacy are acting on questionable moral ground, based on Gewirth's model.

If we look at the issue of privacy through the lens of Gewirth's second necessary condition, that of *well-being*, and consider the established impact of privacy violation on self-esteem, self-respect, self-concept and other important mental health elements, it becomes self-evident that deliberate incursions on an individual's privacy violate the second necessary condition as well.

Related to freedom and well-being, and relevant to privacy, Gewirth also introduces the concept of "additive goods," which, viewed "generically-dispositionally," "consist in the means or conditions that enable any person to increase his capabilities of purpose-fulfilling action and hence to achieve more of his goals," consistent with exercising "his own rights to

freedom and to additive well-being" (1978, pp. 240-242). Gewirth declares that we are obliged "to refrain from interfering with (others) having such conditions," adding, "To interfere with someone in this way is to inflict on him specific harms" (1978, pp. 240-242) and thereby diminish well-being, contrary to Gewirth's second necessary condition. Gewirth also links the concept of *additive goods* to the realization and maintenance of self-esteem and argues that we have a duty to esteem and respect others. Given the known impacts of privacy infringement on self-esteem and on well-being more broadly, and the lack of respect that it embodies, it can reasonably be deduced that Gewirth would find encroachment on privacy to be at odds with his conception of additive goods and, therefore, to be morally problematic.

Moreover, based on Gewirth's assertions, the deliberate breach of the aforementioned necessary conditions constitutes a violation of fundamental human rights, generic rights and moral rights, as defined by Gewirth himself. I have already established that a deliberate infringement on personal privacy qualifies as such a breach; it also constitutes, therefore, a violation of all three categories of rights in the eyes of Gewirth.

Gewirth pronounces "reputation and privacy" to be rights "of all persons" and suggests that the deliberate infringement of such rights should be punishable under criminal law (1978, pp. 294-295). Raising a second type of "goods," Gewirth also categorizes privacy and reputation as "non-subtractive goods," which he defines as something that the bearer views as good and the dispossession of which, or damage to which, would lower "his level of purpose-fulfillment" and capacity for action, and would inflict harm (1978, p. 231). Privacy violations involving identify theft, fraud, or other exploitative use or distribution of personal information can certainly cause harm to an individual and can lower one's capacity for action and level of purpose-fulfillment. Such harm can include, to cite just a very few of a potential

plethora of examples, a marred reputation, damaged human relationships, lost financial means or resources, or reduced self-esteem or self-confidence, all of which have been identified as potential consequences to privacy invasion. The harm can also include a consequent reluctance to use informational or other resources, such as the Internet, cellular phones or even credit cards, in turn causing lost opportunities for the victim. Since intentionally causing harm is morally wrong, according to Gewirth, deliberate privacy invasion, which is known to be harmful, is morally wrong.

Gewirth also introduces a third type of "goods", namely "basic goods", which he describes as "the general necessary preconditions of action" (1978, p.54). These include certain physical necessities of life, such as bodily integrity, food, shelter and clothing, as well as psychological needs, such as "mental equilibrium and a feeling of confidence as to the general possibility of attaining one's goals." Gregory Walters (2001) aptly likens the triumvirate of Gewirth's regime of goods—i.e., basic, non-subtractive and additive—to Maslow's hierarchy of needs, wherein each successive level becomes less grounded in mere physical survival but equally significant for enjoying the full human experience and achieving self-actualization.

Gewirth acknowledges that, while harm caused by the removal, or infringement upon the acquisition or retention, of basic goods is readily condemnable as morally wrong—and this would include privacy invasion based on its known impacts in relation to psychological needs as elaborated above—it can be more challenging to morally judge such actions in regard to non-subtractive and additive goods, given that the nature of such goods can, and does, vary immensely among individuals and circumstances, and that the criteria for a broad potential gamut of harms, therefore, becomes relatively specific and individualized for any

given person or set of circumstances. From an ethical perspective it also becomes somewhat arbitrary. In attempting to address this philosophical challenge, Gewirth offers a more generic and universally applicable approach to judging the morality of a given specific harm "that consists in having one's level of purpose-fulfillment lowered" (non-subtractive; 1978, p.231). He achieves this by drawing a distinction between goods ("particular-occurrent" view), on the one hand, and "capabilities of action" necessary to have them ("generic-dispositional" view), on the other (1978, pp. 54, 58-59, 233). Non-subtractive *capabilities of action* are inherently more generic and universal because they are focused on retaining not what one regards as good, which, as previously noted, varies immensely, but one's undiminished capabilities for particular actions, including the *capacity* to retain what one sees as good. This *capacity* is far more universal and less arbitrary than any individual's specific assortment of perceived goods selected from an almost infinite menu of possibilities. Actions that would universally obstruct or diminish these capabilities within the context of non-subtractive goods are considered to inflict non-arbitrary harms and, therefore, to be immoral (Gewirth, 1978). Gewirth explicitly cites "having one's privacy violated" or interfered with to constitute such harm and therefore to be immoral. Gewirth does not make the argument with respect to *additive* goods that he makes for non-subtractive goods, at least not in specific reference to privacy; however, essentially the same logic and arguments would apply equally well to both, only, in the case of additive goods, rather than focusing on diminished capability, the arguments would focus on prevention of or impediment to *increased* capability. Most importantly, they would lead to the same conclusion—i.e., that privacy invasion, in any form, is almost always morally wrong.

6. Conclusion

In this thesis I set out to validate two assertions in my hypothesis—namely, 1) that privacy as a concept remains highly relevant on both individual and societal levels, and 2) that its restoration and preservation constitutes an ethical imperative. I defended the first assertion by arguing the continued indispensability of privacy from the three perspectives of psychological need, social values and fundamental rights. I established that privacy is vital, not only for the emotional well-being of each and every individual and for the social fabric of society, but also in the very practical interest of the business world itself, which, while possibly the greatest violator of privacy, stands to suffer whenever certain forms of privacy invasion occur, such as identity or password theft, unauthorized disclosure of sensitive financial or account information, credit card compromises, fraud, and so on. I also identified risks and consequences of encroachment on privacy and demonstrated the importance that many key elements of society attribute to privacy. I then built on this line of reasoning to defend the second assertion by presenting supporting arguments from various ethical perspectives as offered by four esteemed philosophers. In so doing, I have hopefully established the ethical inviolability of privacy as a real, meaningful and even practical concept, as well as society's obligation not only to preserve whatever vestiges still remain, but also to endeavour to heal some of its injured dimensions and restore privacy to a state where "privacy by design," much like "security by design," becomes part of our collective psyche such that in the development and implementation of new technologies and applications we not only pay lip service to privacy to create the illusion of respecting it, but meaningfully embrace it in the recognition that its preservation and well-being is both right and in the interest of humankind overall. As former Canadian Privacy Commissioner George Radwanski stated in

his Annual Report to Parliament, 2001-2002, "… privacy—the right to control access to ourselves and to personal information about us—is at the very core of our lives. It is a fundamental human right precisely because it is an innate human need, an essential condition of our freedom, our dignity and our sense of well-being" (Shade, 2008, p. 80).

Further to instilling within ourselves a strong conviction of the real importance of privacy and of the need to re-engineer our collective approach to treating it, there are many practical measures that societies can take toward addressing some of the more acute and immediate concerns and mitigating their impact. While this thesis is not intended to serve as a practical manual for mending privacy ills, I would submit that we need to better protect minors from non-consensual data collection and retention, tracking of online behaviour, profiling, and targeting altogether, as they are the most vulnerable among us. We would also stand to benefit from implementing more aggressive, comprehensive and timely legislation, as well as binding policies, aimed specifically and explicitly at protecting privacy, and from seeking greater consistency in these areas as well as stricter enforcement across jurisdictions, especially internationally. In addition, to quote Leslie Regan Shade, "Privacy rights are intrinsic to communication rights, and policy debates toward recognizing and implementing a Canadian charter should be renewed" (2008, p.90).

Manuel Velasquez (2001) lays out the following guidelines for collecting information about individuals:

1) the purpose of collecting the information must be legitimate;
2) the information collected must be relevant to the purpose;
3) the person about whom information is to be collected must be informed prior to the collection of the information;

4) the party about whom data is being collected must consent to the collection of the data, either implicitly or explicitly;
5) steps must be taken to ensure accuracy of the data; and
6) the recipients of the data must not proliferate and data bases must be secure (so that the data do not get beyond the entity that has a legitimate purpose to collect them and to whom consent to collect it has been given; pp. 365-368).

While there is certainly room for interpretation and, consequently, abuse of the above principles, the spirit of each of them is congruent with the ideologies of Mill, Kant, Rawls and Gewirth, and may well serve as a sound universal foundation upon which to build ethical and legal frameworks and operational policies for future activities involving the gathering and treatment of personal information.

Some loss of privacy may be unavoidable in the information age and in our globalized world. That does not equate, however, to privacy being relegated to the ranks of a philosophical relic or an anthropological artifact of a bygone era, or to the inevitability of its becoming such in time. Moreover, it does not absolve us of our obligation never to abandon the pursuit of privacy. Rather, privacy's unquestionable erosion, particularly over the past few decades, and current trends give cause for serious concern, sober reflection, and collective action, lest societal capitulation allow the trend to continue and privacy to dwindle to a point where it truly is little more than an academic concept. Without proper regard for and treatment of information privacy, and privacy in general, we in the integrated digital world could soon find ourselves in a virtual fishbowl, rendered helplessly and wholly visible to anyone who cares to look, and a little less human as a consequence.

7. References

Allen, A. (1988). *Uneasy Access: Privacy for Women in a Free Society*. Totowa, N.J.: Rowman and Littlefield.

Ashford, E. and Mulgan, T. (2012). Contractualism. *Stanford Encyclopedia of Philosophy* [online]. Retrieved October 1, 2013, from http://plato.stanford.edu/entries/contractualism/

Benn, S. (1971). Privacy, freedom, and respect for persons. In J. R. Pennock & J. W. Chapman (Eds.), *Nomos XIII: Privacy* (pp. 1–26). New York: Atherton Press.

Benn, S. (1978). The protection and limitation of privacy, Part I. *Australian Law Journal,52,* 601–612.

Bercer, F.R. (1979). John Stuart Mill on Justice and Fairness. *Canadian Journal of Philosophy, 9*(1), 115-136.

Bloustein, E. (1964). Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser. *New York University Law Review*, *39*, 962–1007.

Brodkin, J. (2009, December 8). Facebook Halts Beacon, Gives $9.5M to Settle Lawsuit. *PCWorld* [online]. Retrieved September 27, 2013, from http://www.pcworld.com/article/184029/facebook_halts_beacon_gives_9_5_million_to_settle_lawsuit.html

Bushey, W.P. (2011). *An Analysis of Federal Policy on Internet Consumer Privacy and a Study of the Relationship between Privacy, Information, Trust, and Valuation*. Unpublished master's thesis, University of Minnesota.

Center for Democracy and Technology Web site. (2013). Retrieved October 2, 2013, from https://www.cdt.org/privacy/guide/protect/laws.php

Chandler, J. (2009). Privacy Versus National Security: Clarifying the Trade-off. In I. Kerr, V. Steeves and C. Lucock (Eds.), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (pp. 121-138). New York: Oxford University Press.

Christman, J. (2009). Autonomy in Moral and Political Philosophy. *Stanford Encyclopedia of Philosophy* [online]. Retrieved October 11, 2013, from http://plato.stanford.edu/entries/autonomy-moral/

Cohen, J.L. (2002). *Regulating Intimacy: A New Legal Paradigm.* Princeton: Princeton University Press.

Council of Europe. (1950). *Convention for the Protection of Human Rights and Fundamental Freedoms*. Article 8(1). Retrieved September 21, 2013, from http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm

Davies, S.G. (1997). Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity. In P.E. Agre and M. Rotenberg (Ed.), *Technology and Privacy: The New Landscape* (pp.143-165). Cambridge, MA: MIT Press.

DeCew, J. (2013). Privacy. *Stanford Encyclopedia of Philosophy* [online]. Retrieved September 29, 2013, from http://plato.stanford.edu/archives/fall2013/entries/privacy/

Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of

Such Data. (1995). Retrieved September 19, 2013, from http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

Dolman, J., Thomas, E. and Bruschetta, L. (2012, January 23). *Ontario Court of Appeal Recognizes Tort of Invasion of Privacy*. Retrieved November 22, 2013, from http://www.osler.com/NewsResources/Ontario-Court-of-Appeal-Recognizes-Tort-of-Invasion-of-Privacy/

Donner, W. (1991). *The Liberal Self: John Stuart Mill's Moral and Political Philosophy*. Ithaca, New York: Cornell University Press.

Electronic Privacy Information Centre Web site. (2013). *Social Networking Privacy*. Retrieved October 3, 2013 from http://epic.org/privacy/socialnet/

Etzioni, A. (2012). The Privacy Merchants: What is to be done? *The Journal of Constitutional Law*, *14*(4), 950.

Flaherty, D.H. (1999). Some Reflections on Privacy and Technology. *Manitoba Law Journal, 26*(2), 219-233.

Fox, M. (2013, February 22). Alan F. Westin, Who Transformed Privacy Debate Before the Web Era, Dies at Age 83. *New York Times* [online]. Retrieved November 19, 2013, from http://www.nytimes.com/2013/02/23/us/alan-f-westin-scholar-who-defined-right-to-privacy-dies-at-83.html?_r=0

Fried, C. (1970). *An Anatomy of Values.* Cambridge, MA: Harvard University Press.

Garrett, J. (2002). *John Rawls on Moral Principles of Individuals with Emphasis on Implications for Business Ethics*. Retrieved October 18, 2013, from http://people.wku.edu/jan.garrett/320jrpfi.htm

Geist, M. (2013, October 29). Is Bell's plan to monitor its customers' habits legal? *The Ottawa Citizen*, pp. D1-2.

Gerstein, R. (1978). Intimacy and Privacy. *Ethics*, *89*, 76–81.

Gewirth, A. (1978). *Reason and Morality*. Chicago and London: The University of Chicago Press.

Gewirth, A. (1987, May). Moral Foundations of Civil Rights Law. *The Modern Schoolman*, *64*(4), 235-255.

Global Privacy Enforcement Network Web site. (2013). Retrieved November 25, 2013, from https://www.privacyenforcement.net/

Graham, G. (2011). *Theories of Ethics: An Introduction to Moral Philosophy with a Selection of Classic Readings*. London and New York: Routledge.

Gross, G. (2013, October 10). People flock to anonymizing services after NSA snooping reports. *PCWorld* [online]. Retrieved November 25, 2013, from http://www.pcworld.com/article/2054040/people-flock-to-anonymizing-services-after-nsa-snooping-reports.html

Guyer, P. (1998). Kant, Immanuel. In E. Craig (Ed.), *Routledge Encyclopedia of Philosophy*. London: Routledge. Retrieved November 29, 2013, from http://www.rep.routledge.com/article/DB047SECT9

Hann, I.H., Hui, K.L., Lee, T.S. and Png, I.P.L. (2002). *Online Information Privacy: Measuring the Cost-Benefit Trade-off*. Paper presented at the 23rd Annual International Conference on Information Systems. Barcelona, Spain.

Hasselback, D. (2012, January 24). *Ontario Court of Appeal recognizes invasion of privacy as common law tort*. Retrieved November 22, 2013, from http://business.financialpost.com/2012/01/18/ontario-court-of-appeal-recognizes-invasion-of-privacy-as-common-law-tort/

Health Canada gaffe outs up to 40,000 medical marijuana users in letters. (2013, November 22). *CTV News* Web site. Retrieved November 28, 2013, from http://atlantic.ctvnews.ca/health-canada-gaffe-outs-up-to-40-000-medical-marijuana-users-in-letters-1.1555415

Heydt, C. (2006). John Stuart Mill (1806-1873). *Internet Encyclopedia of Philosophy*. Retrieved October 8, 2013, from http://www.iep.utm.edu/milljs/

Hirsch, D. (2010). The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation? *Seattle University Law Review*, *34*(2), 439-80. Retrieved November 24, 2013, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1758078

Hofstede, G. (1991). *Cultures and Organizations: Software of the Mind*. London: McGraw-Hill.

Hollis, G. (2013). *An Evaluation of John Stuart Mill's Harm Principle*. Retrieved October 11, 2013, from http://georginahollis.hubpages.com/hub/AnEvaluationofJohnStuartMillsHarmPrinciple

Horton, S. (2007). Kant on the Primacy of Human Rights. *Harper's Magazine* [online]. Retrieved November 29,2013 from http://harpers.org/blog/2007/08/kant-on-the-primacy-of-human-rights/

Hung, R. and MacIsaac, R. (2013, June 17). *Canada: BC vs Ontario: BC Supreme Court Confirms No Common Law Tort for Invasion of Privacy*. Retrieved November 22, 2013, from http://www.mondaq.com/canada/x/245458/Data+Protection+Privacy/BC+vs+Ontario+BC+Supreme+Court+Confirms+No+Common+Law+Tort+For+Invasion+Of+Privacy

Hurley, M. (2013, January 18). DND violated man's privacy rights, commissioner rules. *The Ottawa Citizen*, pp. A1, A6.

Information Commissioner's Office Web site. (2013). Retrieved October 14, 2013, from http://www.ico.org.uk/about_us

Inness, J. (1992). *Privacy, Intimacy and Isolation*. Oxford; Oxford University Press.

Johnson, D.G. (2009). *Computer Ethics* (4th ed.). Pearson/Prentice Hall.

Kant, I. (1964). *The Metaphysical Principles of Virtue: Part II of The Metaphysics of Morals* (J. Ellington, Trans.). Indianapolis, IN: The Bobbs-Merrill Co., Inc. (Original work published 1797).

Kant, I. (2012). *Groundwork of the Metaphysics of Morals* (M. Gregor & J. Timmermann, Trans.). Cambridge: Cambridge University Press. (Original work published 1785).

Kerr, I., Steeves, V. and Lucock, C. (Eds.). (2009). *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, New York: Oxford University Press.

Koetsier, J. (2013). Bye-bye, Google Buzz (again).VentureBeat [online]. Retrieved November 14, 2013, from http://venturebeat.com/2013/05/27/bye-bye-google-buzz-again/

Kravets, D. (2010, March 17). Judge Approves $9.5 Million Facebook 'Beacon' Accord. *Wired* [online]. Retrieved September 27, 2013, from http://www.wired.com/threatlevel/2010/03/facebook-beacon-2/

Kundera, M. (1984). *The Unbearable Lightness of Being.* New York: Harper Collins.

Laucius, J. (2013, April 5). Hospital finds USB key with patient info. *The Ottawa Citizen*, p. C2.

Lawson, P. and O'Donoghue, M. (2009). Approaches to Consent in Canadian Data Protection Law. In I. Kerr, V. Steeves and C. Lucock (Eds.), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (pp. 23-42). New York: Oxford University Press.

Lax security at Canada Revenue leads to privacy breaches – Privacy watchdog calls on federal agencies to better handle personal information. (2013, October 29). *CBC News* Web site. Retrieved, 28 November, 2013 from http://www.cbc.ca/news/politics/lax-security-at-canada-revenue-leads-to-privacy-breaches-1.2286889

Lessig, L. (2006). *Code: Version 2.0.* New York: Basic Books.

Lucock, C. and Black, K. (2009). Anonymity and the Law in Canada. In I. Kerr, V. Steeves and C. Lucock (Eds.), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (pp. 23-42). New York: Oxford University Press.

Martin, R. and Adam, G.S. (1994). *A Sourcebook of Canadian Media Law*. Ottawa: Carleton University Press.

McFarland, M. (2012). *Why We Care about Privacy*. Retrieved November 15, 2013, from http://www.scu.edu/ethics/practicing/focusareas/technology/internet/privacy/why-care-about-privacy.html

Medical marijuana privacy breach sparks lawsuit. (2013, November 26). *CBC News* Web site. Retrieved November 28, 2013, from http://www.cbc.ca/news/canada/nova-scotia/medical-marijuana-privacy-breach-sparks-lawsuit-1.2440300

Mendez, F. and Mendez, M. (2009). Comparing Privacy Regimes: Federal Theory and the Politics of Privacy Regulation in the European Union and the United States. *The Journal of Federalism, 40*(4), 617-645. Retrieved November 24, 2013, from http://publius.oxfordjournals.org.proxy.bib.uottawa.ca/content/40/4/617.full.pdf+html

Mill, J.S. (1859). *A Few Words on Non-Intervention*. Retrieved April 24, 2013, from http://www.libertarian.co.uk/lapubs/forep/forep008.pdf

Mill, J.S. (1862). *Considerations on Representative Government*. Retrieved November 28, 2013, from

http://www.heinonline.org.proxy.bib.uottawa.ca/HOL/Index?index=cow%2Fconsorg&collection=cow

Mill, J.S. (1869a). *On Liberty.* London: Longman, Roberts & Green. Retrieved September 8, 2013, from http://www.bartleby.com/130/

Mill, J.S. (1869b). *The Subjection of Women*. Retrieved November 27, 2013, from http://www.constitution.org/jsm/women.htm

Mill, J.S. (1871). *Utilitarianism*. Retrieved August 18, 2013, from http://fair-use.org/john-stuart-mill/utilitarianism/

Millar, J. (2009). Core Privacy: A Problem for Predictive Data Mining. In I. Kerr, V. Steeves and C. Lucock (Eds.), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (pp. 103-119). New York: Oxford University Press.

Moore, A. (1998). Intangible Property: Privacy, Power, and Information Control. *American Philosophical Quarterly*, *35*, 365–378.

Moore, A. (2000). Employee Monitoring & Computer Technology: Evaluative Surveillance v. Privacy. *Business Ethics Quarterly*, *10*, 697–709.

Moore, A. (2003). Privacy: Its Meaning and Value. *American Philosophical Quarterly*, *40*, 215–227.

Moore, A. (2010). *Privacy Rights: Moral and Legal Foundations*. University Park, PA: Penn State University Press.

NSA review panel findings: Liberty and Security in a Changing World. (2013, December 18). *The Guardian* [online]. Retrieved December 19, 2013, from http://www.theguardian.com/world/interactive/2013/dec/18/nsa-review-panel-report-document

Office of the Australian Information Commissioner Web site. (2013). Retrieved October 1, 2013, from http://www.oaic.gov.au/privacy/privacy-act/the-privacy-act

Office of the Information and Privacy Commissioner, Ontario, Canada Web site. (2013). Retrieved May 19, 2013, from http://www.ipc.on.ca/english/privacy/introduction-to-pbd/

Office of the Privacy Commissioner for Personal Data, Hong Kong, China Web site. (2013). *An Overview of the Principles Established by the APEC Privacy Framework.* Retrieved October 2, 2013, from http://www.pcpd.org.hk/english/files/infocentre/1tonylam1_ppt.pdf

Office of the Privacy Commissioner of Canada Web site. (2010). Retrieved May 17, 2013, from http://www.priv.gc.ca/media/nr-c/2010/nr-c_100217_e.asp

Office of the Privacy Commissioner of Canada Web site. (2013a). Retrieved April, 13, 2013, from http://www.priv.gc.ca

Office of the Privacy Commissioner of Canada Web site. (2013b). Retrieved September 9, 2013, from http://www.priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp

Onn, Y., Geva, M., Druckman, Y., Zyssman, A., Timor, R. Lev, I., et al. (2005). *Privacy in the Digital Environment*. Elkin-Koren, N. & Birnhack, M. (Eds.). Haifa Center of Law & Technology.

Open University Web site. (2011). Retrieved September 30, 2013, from http://www.open.edu/openlearn/society/the-law/privacy-rights-and-the-law/content-section-0

Organisation for Economic Co-operation and Development (OECD) Web site. (2013a). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.

Retrieved May 3, 2013, from http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Organisation for Economic Co-operation and Development (OECD) Web site. (2013b). *OECD Privacy Principles*. Retrieved September 30, 2013, from http://oecdprivacy.org/

Pagliery, J. (2013, December 4). 2 million Facebook, Gmail and Twitter passwords stolen in massive hack. *The Cybercrime Economy, CNN* [online]. Retrieved December 7, 2013 from http://money.cnn.com/2013/12/04/technology/security/passwords-stolen/

Parent, W.A. (1983). Privacy, Morality and the Law. *Philosophy and Public Affairs*, *12*, 269–288.

Perez, J.C. (2007, November 30). Facebook's Beacon More Intrusive than Previous Thought. *PCWorld* [online]. Retrieved September 27, 2013, from http://www.pcworld.com/article/140182/article.html

Posner, R.A. (1981). *The Economics of Justice*. Cambridge, MA: Harvard University Press.

Press, J. (2013, January 18). Tories ponder data protection. *The Ottawa Citizen*, p. A2.

Press, J. (2013, January 19). Identity thefts reported. *The Ottawa Citizen*, p. A6.

Press, J. (2013, January 22). HRSDC bans external drives after data breach. *The Ottawa Citizen*, p. A3.

Rachels, J. (1975). Why Privacy is Important. *Philosophy and Public Affairs*, *4*, 323–333.

Rauscher, F. (2007). Kant's Social and Political Philosophy. *Stanford Encyclopedia of Philosophy* [online]. Retrieved September 9, 2013, from http://plato.stanford.edu/entries/kant-social-political/

Rawls, J. (1971). *A Theory of Justice*. Cambridge, MA: Belknap Press of Harvard University.

Regan, P. (1995). *Legislating Privacy*. Chapel Hill, NC: University of North Carolina Press.

Rogers, B. (2002, November 27). John Rawls. *The Guardian*. Retrieved October 12, 2013, from http://www.theguardian.com/news/2002/nov/27/guardianobituaries.obituaries

Rosen, J. (2010, July 21). The Web Means the End of Forgetting. *New York Times*.

Schoeman, F. (Ed.). (1984). *Philosophical Dimensions of Privacy: An Anthology*. Cambridge: Cambridge University Press.

Schoeman, F. (1992). *Privacy and Social Freedom*. Cambridge: Cambridge University Press.

Shade, L.R. (2008). Reconsidering the Right to Privacy in Canada. *Bulletin of Science, Technology & Society*, *28*(1), 80-91.

Solove, D. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, *154*, 477–564.

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

Steeves, V. (2009). Reclaiming the Social Value of Privacy. In I. Kerr, V. Steeves and C. Lucock (Eds.), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (pp. 191-208). New York: Oxford University Press.

Stevens, N. (2010, April). Online Trust & Internet Entrepreneurs: A Kantian Approach. *Wharton Research Scholars Journal.* University of Pennsylvania. Retrieved October 21, 2013, from http://repository.upenn.edu/wharton_research_scholars/60/

Uteck, A. (2009). Ubiquitous Computing and Spatial Privacy. In I. Kerr, V. Steeves and C. Lucock (Eds.), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (pp. 83-102). New York: Oxford University Press.

Velasquez, M.G. (2001). *Business Ethics: Concepts and Cases* (5th ed.). Prentice Hall.

Walters, G.J. (2001). *Human Rights in an Information Age: A Philosophical Analysis*. Toronto, ON: University of Toronto Press.

Warren, S. & Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review*, *4*, 193–220.

Wasser, L.A. (2013, February). *Ontario Court of Appeal recognizes new tort for invasion of privacy*. Retrieved November 22, 2013, from http://www.mcmillan.ca/Ontario-Court-of-Appeal-recognises-new-tort-for-invasion-of-privacy

Westin, A. (1967). *Privacy and Freedom.* New York: Atheneum.