Understanding Privacy Problems
&
Developing Sustainable Solutions:
An Examination of the DNCL initiative in Canada

by
Rebecca Johnston, B.A.(H), B.ED.

A thesis submitted to
the Faculty of Graduate Studies and Research
in partial fulfillment of
the requirements for the degree of

Masters of Arts

Department of Legal Studies
Carleton University
Ottawa, Ontario
April 20, 2009

©2009, Rebecca Johnston

Library and
Archives Canada

Published Heritage
Branch

395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque et
Archives Canada

Direction du
Patrimoine de l'édition

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence
ISBN: 978-0-494-51980-6
Our file Notre référence
ISBN: 978-0-494-51980-6

NOTICE:

The author has granted a non-exclusive license allowing Library and Archives Canada to reproduce, publish, archive, preserve, conserve, communicate to the public by telecommunication or on the Internet, loan, distribute and sell theses worldwide, for commercial or non-commercial purposes, in microform, paper, electronic and/or any other formats.

The author retains copyright ownership and moral rights in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

AVIS:

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque et Archives Canada de reproduire, publier, archiver, sauvegarder, conserver, transmettre au public par télécommunication ou par l'Internet, prêter, distribuer et vendre des thèses partout dans le monde, à des fins commerciales ou autres, sur support microforme, papier, électronique et/ou autres formats.

L'auteur conserve la propriété du droit d'auteur et des droits moraux qui protègent cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

In compliance with the Canadian Privacy Act some supporting forms may have been removed from this thesis.

Conformément à la loi canadienne sur la protection de la vie privée, quelques formulaires secondaires ont été enlevés de cette thèse.

While these forms may be included in the document page count, their removal does not represent any loss of content from the thesis.

Bien que ces formulaires aient inclus dans la pagination, il n'y aura aucun contenu manquant.

Canada

Abstract

The thesis asserts that conventional unilateral approaches to personal information protection are not sufficient to protect personal privacy. The work of Daniel Solove is used to illustrate a contextual, problem-based approach to privacy that side-steps traditional theoretical quagmires. The failure of the private sector to respond, the relative inability of individuals to protect their own information and lack of legislative compliance provides evidence of how current governance assumptions do not provide a foundation for realistic privacy protection. An examination of the DNCL initiative reveals legislative and technological shortcomings compounded by an inadequate process. By recognizing the importance of a sustainable governance approach and evolving towards a more sophisticated and mature, systematic, multi-variable, multi actor approach, a second-generation DNCL solution is possible. Adopting innovative institutions, instruments, and processes found in the other areas could provide specific improvements. The full inclusion of robust civil society organizations is fundamental to any meaningful improvements.

Acknowledgements

I would like to thank Kernaghan Webb who started me on this academic journey and Vince Kazmierski who brought me safely home. I am deeply grateful to Mike Gurski and all the incredible privacy cognoscenti I had the privilege of learning from through The Privacy Network initiative. Finally, my heartfelt love and thanks to Stefan, Eric, Thea and Marnie who encouraged and supported me over the years.

Table of Contents

Abstract	ii
Acknowledgements	iii
Table of Contents	iv
List of Diagrams	v
List of Appendices	vi
Chapter One: Introduction	1
Chapter Two: Identifying Consumer Privacy Problems	8
(Mis) Perceptions of the Privacy Problems	8
Understanding Privacy with Daniel Solove	11
Taxonomy of Privacy Problems	19
Chapter Three: Maturing a Privacy Governance System	26
Evidence of Immature Privacy Governance System	31
Business and Information Protection Technology	31
Government and Legislation	42
The Individual and Individual Capacity	58
Solving the Problem with Sustainable Governance	69
Chapter Four: Case Study - Canadian National Do Not Call List	81
Context of the Process and Development	83
Identifying Consumer Privacy Problems in Relation to Telemarketing using Solove	94
Failure of the current DNCL response	101
Chapter Five: Sustainable Governance lessons for the DNCL	137
Reference List	152

List of Diagrams

Diagram 1 – Model of Taxonomy	p. 21
Diagram 2 – Sustainable Governance: Consumer Protection in Canada	p. 30
Diagram 3 - Data Supply Chain	p. 65

List of Appendices

Appendix A – CSA / PIPEDA Principles	p. 149
Appendix B – Telemarketing Chronology in Canada	p. 150

Chapter One: Introduction

The topic of consumer privacy has continued to rise in public concern in the last decade.¹

The development of the internet, e-commerce and the information economy has brought the business practices of personal information collection, use and dissemination under increasing scrutiny from both the general public and government. Identity theft, fraud, discrimination, profiling, telemarketing and spam are all issues that have emerged. The current generation of internet users are children of the Internet age: weaned on Napster, trained on Google and graduated on Facebook. Few young adults today can conceptualize what life was like before the availability of computerized distributed networks of information. The social or business conventions were not written or understood. Quite the contrary, the Internet has changed and is continuing to change the business, social and legal rules, the players and the game to such a degree that few people truly understand all the underlying contexts, if indeed any single person could. With the amount of money at stake as well as fundamental rights under jeopardy, personal information protection has emerged as an important issue.

The specific threats of privacy violations are not all known, understood or agreed upon. The economic crimes associated with identity theft and associated fraud can sometimes be loosely quantified by dollars lost by consumers. Theft or misuse of personal

¹ Robert L. Scheier, "Your data's less safe today than two years ago" *Computerworld*, online: <<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9031104&pageNumber=4>>.

information is directly associated with mortgage and title fraud², credit card fraud and debit card skimming.³ Employers are increasingly researching their employees as well as clients on the internet.⁴ Recently in Canada, two people running for political office were forced to resign after videos of them surfaced on the internet.⁵ At last count, which is acknowledged to be incomplete, there are over one million victims of fraud each year in Canada and the amount that perpetrators gain from victims is over \$3 billion.⁶

Surveillance and social sorting can lead to discrimination. Last year a man with excellent credit history was denied a loan based on his postal code near an aboriginal reserve.⁷ The psychological harm, inconvenience, discrimination, implications on freedom of speech or democratic participation accompanying perceived personal privacy violations are all less understood or quantifiable.

Given the widespread adoption of information technology and increase in the private sector information economy, how can personal information be best protected? The goal of this thesis is to critically examine both the current and potential ways in which governments, the private sector, civil society and individuals interact to protect or

² CBC News, "Due diligence: The growing problem of mortgage fraud" *CBC News* (9 November 2006), online: <<http://www.cbc.ca/news/background/mortgage-fraud>>.

³ Public Safety Canada, "Advice for consumers Identity theft", online: <<http://www.publicsafety.gc.ca/prg/le/bs/consumers-en.asp>>.

⁴ Ian Shapira, "When Young Teachers Go Wild on the Web Public Profiles Raise Questions of Propriety and Privacy" *Washington Post* (28 April 2008) Page A01, online: <<http://www.washingtonpost.com/wp-yn/content/article/2008/04/27/AR2008042702213.html>>.

⁵ Chad Skelton, "Another B.C. NDP candidate resigns after marijuana video surfaces" *Vancouver Sun* (19 September 2008), online: <<http://www2.canada.com/vancouversun/news/story.html?id=a61b51a4-bace-4fef-8feb-814d67e12b61>>.

⁶ Susan Sproule & Norm Archer, "Measuring Identity Theft in Canada: 2006 Consumer Survey - Working Paper #21" (2006), online: <<http://www.merc-mcmaster.ca/working-papers/measuring-identity-theft-in-canada-2006-consumer-survey/>>.

⁷ Don Butler, "Part II: Devil in the details When it comes to social sorting, you are what you eat, buy, surf, post" *Ottawa Citizen*, (5 February 2009) online: <<http://www.ottawacitizen.com/Business/Part+Devil+details/1232337/story.html>>.

threaten the collection, use and disclosure of the personal information of individuals by commercial entities. This examination will contribute to the development of a realistic, practical and solutions-based multi-partite, multi-variable "sustainable governance" model of protecting personal information.

The main argument of this paper is two-fold. First, in order to create effective privacy solutions that can be deployed on the ground, the basic privacy problems must be clearly articulated and understood. Too often discussions of privacy have digressed down myriad paths of theoretical, legal or data protection rhetoric. Privacy issues have often been complicated by a perceived need to balance against business efficiency, security or law enforcement mandates. In chapter two of the thesis consumer privacy will be placed in a realistic problem-specific context following Daniel Solove's Taxonomy of Privacy.

In chapter three I will illustrate that the failure to protect against or resolve the types of privacy problems identified in chapter two results from governance failures. I argue that this is in part due to three consistent, but misguided, beliefs that have overshadowed the modern privacy governance discourse in Canada. Evidence will also be presented to illustrate some of the identified weaknesses that underlay these mistaken beliefs. First, there is the belief that the business sector has the potential to respond to emerging privacy issues and opportunities at a more rapid pace. The word of note is potential. Chapter three demonstrates that business has not only failed to innovate to protect personal privacy; on the whole, business has acted to further erode it. Businesses have not stepped

up to develop accessible consumer privacy enhancing technologies. There has not been the creation of robust privacy technology standards and architectures.

Chapter three will also examine the role of the individual standing in the cross-hairs of the multitude of businesses, governments and social lenses. Modern liberal capitalist discourse indicates that individuals are the masters of their (internet?) domains and empowered to make their own decisions. Certainly, individuals have the most motivation to protect their information. The reality is much less optimistic. Research into consumer behaviour and behavioural economics reveals that consumers do not always act in their own best interest, nor do they always behave in the most rational ways.⁸ Unfortunately, even if an individual is reasonably conscientious about their data bread crumb trail, recent research into the data broker industry reveals how little control the individual has over how their personal information is collected, shared, and used by numerous organizations with direct relationship to them, thus leaving them vulnerable at innumerable levels.

Finally, the role of government legislation in protecting the privacy of consumers will be considered. Governments are routinely called upon by citizens to use their favourite and dominant instrument - legislation - to resolve social issues. While legislation is a powerful and credible tool, it has become apparent that it is often simply not effective on its own. Chapter three will explore how recent research into the implementation of *PIPEDA* indicates rampant non-compliance. Legislative gaps and jurisdictional roadblocks are a few other examples of legislative limitations. Governments appear to be

⁸Mathew Rabin, "A Perspective on Psychology and Economics" (Working Paper No. E02-313 Department of Economics, University of California, February 2002), online: <http://repositories.cdlib.org/cgi/viewcontent.cgi?article=1003&context=iber/econ>.

toothless tigers against most recent technology issues and are often viewed by critics as being in the pocket of business and industry lobbyists.

In view of fast-changing technologies and variable capabilities of governments, the private sector, civil society, and individuals, conventional unilateral or "single actor"-based approaches to personal information protection are not sufficient to protect personal information or privacy. The privacy governance actors, instruments, institutions and processes as they exist today are weak, fragmented or insufficient. In the attempt to respond to consumer privacy issues, business, legal and technical privacy protections have been developed and implemented in an inconsistent, patchwork fashion. Current responses have largely failed to provide adequate consumer privacy protection.

Kernaghan Webbs' vision of a sustainable governance model will be discussed as a potential approach to effectively resolve privacy problems generated by the collection, use and disclosure of personal information by commercial entities. Each actor has unique and overlapping capabilities, instruments, institutions and processes at their disposal as well as different motivations or incentives for protecting personal information. Each actor also has inherent limitations, disincentives or barriers to the protection of individual privacy. This thesis argues that no single solution has been able to adequately resolve consumer privacy problems in a proactive, efficient, timely or comprehensive way. A sustainable governance model would value a collaborative approach and involve each actor, instrument, institution and process so as to build a mutually reinforcing set of solutions.

The evidence of the immaturity of the existing governance system illustrates the need for a new approach to privacy protection. Following a sustainable governance approach gives consumers the best protection because solutions are designed to capture the strengths of each actor, instrument, instrument and process while compensating for the inherent weaknesses. A sustainable governance approach will improve consumer privacy protection by addressing the specific weaknesses of a failure of the business sector to respond, weakness of individuals to protect themselves and strengthen the responses implicated through legislation and regulation.

In chapter four, the Canadian National Do Not Call List case study will be used as a concrete example to illustrate the processes engaged to define and then address the specific privacy issues around telemarketing. I will demonstrate how the current privacy governance approach failed to adequately understand the fundamental privacy problems caused by the collection, use and disclosure of personal information in telemarketing. In addition, I will examine how the process engaged and the actors and institutions involved were insufficient to compensate for the fundamental misunderstanding of the nature of the problems resulting in an ineffective solution.

In chapter five an argument will be made that implementing a sustainable governance approach may potentially compensate for inherent weaknesses in the process and create a system that substantially improves consumer privacy protection. Several practical as well

as innovative suggestions will be made as to how a next generation, version 2.0 DNCL solution could be envisioned.

Ultimately, this thesis will argue that in order to solve a privacy problem, that problem must be first clearly and pragmatically identified and understood. Secondly, solving the privacy problem involves designing inclusive solutions that recognize and respond to the strengths and weaknesses of all the actors, instruments, institutions and processes implicated by the problem.

Chapter Two: Identifying Consumer Privacy Problems

This chapter will outline the first part of the theoretical framework used in the thesis.

The concept of privacy encompasses multiple dimensions and spans multiple disciplines.

In the policy realm, this conceptual complexity has led to a great deal of confusion in understanding the issues involved and has interfered with attempts to develop practical and effective solutions to specific problems. The work of legal theorist Daniel Solove will be used to define a practical conceptualization of privacy and privacy problems. In turn, in chapter three, the work of Kernaghan Webb will be considered as a framework for developing responses to privacy problems.

(Mis) Perceptions of the Privacy Problems

There is a sense that there is a systemic and increasing privacy problem in Canada and internationally. The exact scope and nature of the privacy problem is difficult to understand and quantify. More business and services are being conducted online than ever before. Consumers increasingly expect to be able to receive information and perform actions online. They appreciate the conveniences associated with online services. However, there are almost daily reports of data breaches each one larger and involving

more records than the last. There have been breaches of employment websites,⁹ credit card payment services¹⁰, and government offices.¹¹

There has also been a dramatic expansion of the role of the internet from simply a commercial or business utility to be used as a broader social tool. Facebook, MySpace and Flickr are examples of commercial social networking sites that encourage and facilitate the sharing of personal information. Facebook, the largest social networking site used in Canada, has reported over 150 million users making it the equivalent to the 8th most populous country in the world.¹² Many users have reconnected with lost friends and enjoyed the ability to remain connected to current friends. There have been several high profile issues regarding Facebook including their launch of a service that publicly posted a users' recent purchases.¹³ Additionally, a recent court case in Ontario has deemed that information posted on Facebook sites is considered to be producible as "documents" under discovery and subject to cross-examination regardless of the users' privacy settings.¹⁴

The media is increasingly reporting on government surveillance of citizens including the use of consumer personal information gained from private businesses in the name of

⁹ Elinor Mills, "User data stolen from job site Monster" *CNET News* (26 January 2009), online: <http://news.cnet.com/8301-1009_3-10149884-83.html>.

¹⁰ Elinor Mills, "Payment processor Heartland reports breach" *CNET News* (20 January 2009), online: <http://news.cnet.com/8301-1009_3-10146275-83.html>.

¹¹ Tom Espiner, "U.K.'s Home Office admits to database breaches" *CNET News* (31 August 2006), online: <http://news.cnet.com/U.K.s-Home-Office-admits-to-database-breaches/2100-1029_3-6111358.html?tag=mncol>.

¹² Julie Smith, "Facebook Growth Continuing, Surpasses 150 Million Monthly Active Users" *Inside Facebook* (7 January 2009), online: <<http://www.insidefacebook.com/2009/01/07/facebook-growth-continuing-surpasses-150-million-monthly-active-users/>>.

¹³ Facebook Press release, "Leading Websites Offer Facebook Beacon for Social Distribution" (6 November 2007), online: <<http://www.facebook.com/press/releases.php?p=9166>>.

¹⁴ *Leduc v. Roman*, 2009 Canlii 6838 (ON S.C).

national security and anti-terrorism. Under the *USA Patriot Act*¹⁵, the US government can compel the release of personal consumer information held by private sector companies.¹⁶ In Canada, there have been two attempts to introduce Lawful Access legislation which would facilitate security and law enforcement access to consumer data including online records.¹⁷

The benefits of information, communication and social technology services are evident. However, the risks to individuals are increasing as more personal information is being shared with more networks, companies and locations. There are constant public reminders to be vigilant against commercial credit fraud, cyber stalking and identity theft. But are these activities privacy violations, civil rights abuses or information technology management issues? Are these breaches of trust or criminal activities? Is the problem one of surveillance or balancing security requirements? At its most basic level, the issues ask us to define ‘what is privacy’? Exactly what are the ‘problems’ that trouble us? What level of privacy do we expect? Can we or do we all have to have the same expectations of privacy? Legal or theoretical works usually begin by outlining the definition of privacy used. Unfortunately, there is no consensus, common definition of the issue or unifying approach. Everyone approaches the ‘privacy problem’ with his or her own perspective, framework or context. The emerging data about potential privacy problems is therefore

¹⁵ *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* [US PATRIOT ACT], Pub. L. 107-56, 272 Stat. 115 (2001), online: <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107>.

¹⁶ EPIC, “The USA PATRIOT Act”, online: <<http://epic.org/privacy/terrorism/usapatriot/>>.

¹⁷ Canadian Internet Policy and Public Interest Clinic, “Lawful Access: Police Surveillance”, online: <<http://www.cippic.ca/lawful-access/#LA21>>.

limited, inconsistent or simply unavailable. There are no common metrics, evaluation criteria or benchmarks by which privacy can be defined or measured.

Understanding Privacy with Daniel Solove

Business author Mikel Harry states:

“Trying to improve something when you don’t have a means of measurement and performance standards is like setting out on a cross-country trip in a car without a fuel gauge. You can make calculated guesses and assumptions based on experience and observations, but without hard data, conclusions are based on insufficient evidence.”¹⁸

Henry’s observation is particularly apt where privacy issues are concerned. Without a common conception of what is at stake, it is difficult to design appropriate solutions. In his recent book *Understanding Privacy*, legal theorist Daniel Solove puts forward a new theory of privacy that seeks to break free from the conceptual quagmire that currently impedes the development of effective policy to deal with privacy issues.¹⁹ Solove’s theory diverges from the traditional, but limited legal conceptions of privacy such as the right to be let alone, limited access to the self, control over personal information and secrecy. *Understanding Privacy* illustrates the shortcomings of the traditional privacy theories in order to conclude that privacy as a concept does not lend itself to traditional or essential elements. Solove believes that many conceptions of privacy in use today are simultaneously too broad or too narrow to be of practical use.

The first conception of privacy that Solove dispels is one of the oldest legal privacy theories asserted by American lawyers Warren and Brandeis in their article “The Right to

¹⁸ Mikel Harry & Richard Schroeder, *Six Sigma: The Breakthrough Management Strategy Revolutionizing the World's Top Corporations* (New York: Doubleday Business, 1999).

¹⁹ Daniel Solove, *Understanding Privacy* (Cambridge: Harvard University Press, 2008).

Privacy” published in 1890.²⁰ Their position condenses into an assertion of the legal right of privacy defined as ‘the right to be let alone.’ It is generally accepted that this foundational law review article shaped most of the privacy legal theory, constitutional and statutory legislation and tort actions to date in the United States.²¹ This concept has resonated both in popular culture and popular privacy discourse in both the United States and Canada. In 1967, the Fourth Amendment of the US constitution, which sets out the protection against unreasonable search and seizure, was interpreted to include the “right to privacy” using the Warren and Brandeis argument.²² The Warren and Brandeis doctrine came to be understood in society that people should be able to live their lives, “as one chooses, free from assault, intrusion or invasion.”²³ Further extensions of the doctrine expanded the right of privacy to include the right of the individual to, “shape his own life as he thinks best, do what he pleases, go where he pleases.”²⁴

However, Solove points out that the right to privacy, like every other right is not absolute, and there is little direction in this doctrine that provides practical guidelines and parameters. According to Solove, “Understanding privacy as the right to be let alone does not inform us about the matters in which we should be let alone.”²⁵ Bennett and Rabb have also noted specific feminist criticisms of the Warren and Brandeis argument which was seen to be used to advocate for traditional male power and autonomy in the home

²⁰ Warren, Samuel and Louis Brandeis, “The Right to Privacy” 4 Harvard Law Review 193 (1890), online: <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>.

²¹ Solove, *supra* note 19 at 89.

²² *Ibid.* at 162.

²³ *Ibid.* at 17.

²⁴ This principle has become a cornerstone of western democracies and forms the basis for the interpretation of Forth Amendment to include protection of the right to abortion.

²⁵ Solove, *supra* note 19 at 17.

and contributed to the continued subjugation of women.²⁶ Further, the US constitution was framed as a document that protects the individual from the state and does not apply directly to the actions of individuals or corporations.²⁷ There is no general federal commercial privacy legislation in the United States as privacy is dealt with federally on a sector-by-sector basis. Thus, a consumer doesn't have the protection of an overarching federal privacy law outlining a specific 'right to privacy' against a business or other individual. There is no federally consistent assistance in this conception for a consumer who wants to make a purchase online but not have their data resold to a data broker and there is no protection against privacy violations of another individual.

In Canada there is no specific mention of privacy in the *Charter of Rights and Freedoms*.²⁸ However, the Supreme Court of Canada has determined in the 1984 *Hunter v. Southam* decision that individuals have a reasonable expectation of privacy in some contexts under Section 8, which protects against unreasonable search and seizures.²⁹ What constitutes reasonable is not completely articulated and is constantly being redefined. Some members of the Court have also identified section 7 as a source of protection of privacy.³⁰ However, it is important to note that, the Canadian *Charter* applies only to citizens in relation to the government, not other individuals or businesses. Similarly, the federal *Privacy Act* focuses on protection against invasion of privacy by

²⁶ Colin Bennett and Charles Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*. (Cambridge: MIT Press, 2003), at 15.

²⁷ *United States v. Jacobsen*, 466 U.S. 109 (1984) online: <<http://supreme.justia.com/us/466/109/case.htm>>.

²⁸ *Canadian Charter of Rights and Freedoms, Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11.

²⁹ *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145. Privacy rights can also be protected through the *Privacy Act* (which protects against invasion of privacy by government) and by statutory invasion of privacy torts in some provinces.

³⁰ See, for example, *R. v. O'Connor*, [1995] 4 S.C.R. 411; *M.(A). v. Ryan*, [1997] 1 S.C.R. 157.

government. *PIPEDA*, the commercial privacy legislation does not protect against privacy violations from other individuals although statutory invasion of privacy torts provide some protection in some provinces.

Privacy can also be viewed as a form of secrecy. This is understood broadly as the right to conceal information about the self; privacy is violated when information is disclosed against the wishes of the subject. Privacy as secrecy has come to be understood in the US as an ‘all or nothing’ proposition meaning once a fact has been disclosed the information is no longer considered private.³¹ Similarly, citizen expectations of privacy have been challenged based on the degree to which the citizen willingly exposed themselves to the public. Judicial decisions have determined the lack of personal privacy rights in garbage set at the curb and allowed for surveillance following this logic.³² In Canada, the 2004 Supreme Court of Canada decision *Tessling* determined that once personal information emanated into the public sphere there was no longer a reasonable expectation of privacy.³³ Professor Ian Kerr has noted several flaws in the *Tessling* decision. He posits that this decision has negative implications for privacy particularly with the increase in technologies from which individuals cannot reasonably protect themselves.³⁴

The current conception of privacy as secrecy can be argued as being too narrowly interpreted. Most notably, in recent years an argument has been raised that this

³¹ *Katz v. United States*, 389 U.S. 347 (1967).

³² *R. v. Patrick*, 2009 SCC 17. [2009]

³³ *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432,. In this case heat emanations from Tesslings’ home were being used to investigate the possibility of a marijuana grow operation.

³⁴ Ian Kerr, Max Binnie & Cynthia Aoki, “Tessling on my Brain: The Future of Lie Detection and Brain Privacy in the Criminal Justice System”, *Canadian Journal of Criminology and Criminal Justice*, (Forthcoming 2008), online: <http://iankerr.ca/images/stories/tessling_on_my_brain.pdf>.

conception as it is currently framed fails to encapsulate the nuances of group privacy or privacy in social networks. For example, a son may reveal to his friends that he got really drunk at a party the night before but he doesn't want his parents to know. An argument can be made that the son has a reasonable expectation to keep the information a secret from his parents even though others know. Most privacy as secrecy concepts cannot comfortably coexist with selective secrecy / privacy situations. Is a secret a secret if many people know? Solove asserts that as social creatures people should have an expectation of privacy in public. Consumers provide their address to a company in order to facilitate shipping their purchase. As such, the consumer would not have an expectation of privacy from the company. However, a consumer should be able to have that information kept private from that company's affiliates or marketers if they so chose. According to Solove, secrecy as the common denominator of privacy is also an insufficient conception because it results in a definition that is too narrow to be useful and fails to provide practical guidance.

Alan Westin provided one of the most relied upon definitions of privacy in his 1967 book *Privacy and Freedom*.³⁵ Westin's definition of privacy has been used to frame the discussion over the past 40 years.

Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.³⁶

³⁵ Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1967).

³⁶ *Ibid.* at 7.

Westin believes that personal information, “thought of as the right of decision over one’s private personality” would be best viewed as a property right giving the individual legal control over their information. Personal information or attributes are viewed as an extension of personality that belongs to the individual. A consumers’ address therefore is a piece of information that belongs to the consumer. Taking that information without permission could be viewed as a theft of property. Westins’ approach follows a traditional liberal ideal of privacy that elevates the private property rights of the individual. Solove, among others, has advanced specific criticisms of Westins’ privacy as control over personal information or property argument.

Solove illustrates several shortcomings when viewing personal information as property. First, not all privacy issues can be reduced to informational facts. For example, the freedom to make bodily decisions or lifestyle choices aren’t commodifiable. Similarly, knowledge of personal information doesn’t always exist solely in tangible, exchangeable form. Multiple people can be in possession of the same information and once someone knows the information they can’t necessarily give it back.

Solove is not alone in critiquing Westin and the dominant liberal conception of privacy. In her book, Priscilla Regan has also criticized Westins’ conception of privacy. Regan has argued that the liberal framework views privacy as an individual right which assumes a conflict between the individual and the broader social good. She asserts that a market-based solution for privacy is not effective. She argues that third-party record holders operate under a double standard because they wish to treat the information as a

commodity but not inform or compensate the public regarding the sale of personal information. Regan indicates that many information exchanges are non-voluntary and often individuals cannot avoid disclosing some information. She also notes that the designers of the information communication technologies (ICTs) themselves claim that it is too difficult to differentiate levels of privacy for different people. Recognizing this, how then would the monetary value of the information be quantified in a system of exchange? In her analysis, Regan concludes that privacy “is becoming less an attribute of individuals and records and more an attribute of social relationships and information systems or communication systems.”³⁷

Solove’s work serves to illustrate the point that traditional conceptions of privacy are not sufficiently nuanced to address the real problems facing individuals in the age of telecommunications and hyper-security. Existing laws and jurisprudence may no longer be appropriate given the changes in technology and its implications.

After dispelling these and several other privacy conceptions and theories, Solove sets forward a framework that is grounded in specific contexts and focused on the “privacy problems”.³⁸ Solove argues that attempting to define the core elements and characteristics of privacy has not only been unsuccessful, it has hindered the overall understanding of the concept. He asserts that privacy must be understood as a pluralistic concept rather than as a single unifying theory with a common denominator. His work recognizes that there are different attitudes and realities that impact how privacy is viewed and therefore

³⁷ Priscilla Regan, *Legislating Privacy* (Chapel Hill: University of North Carolina Press, 1995).

³⁸ Solove, *supra* note 19 at 9.

addressed. Building on Wittgensteins' theory of family resemblances, Solove's theory validates privacy as a concept that includes a variety of different, yet related, concepts. According to Solove, privacy issues have many differences and lack a single or common denominator and a 'resemblances' theory accommodates different conceptions of privacy. He believes that any theory must be general enough to provide some degree of transference without becoming too broad so as to address specific, practical issues. He understands that there are numerous cultural, social, historical and practical variations in how privacy is conceptualized.

Solove illustrates evolving attitudes towards privacy in specific contexts. For example, nudity and the human body was viewed in Ancient Greece and Rome as a symbol of pride and civility with citizens often exercising or bathing together in the nude in contrast with Victorian notions of female modesty. The modern western culture of exhibitionism perhaps indicates a middle ground in the public perspective. Attitudes and approaches to bodily functions and sexuality have also diverged across history and cultures. Up until the seventeenth century, whole European families shared one-room cottages where bodily privacy was near impossible or impractical. Solove notes concepts of bodily privacy emerged in western society as larger homes were built and more single purpose rooms created. Anthropologists have documented tribal societies for whom there is little or limited notions of bodily privacy but nonetheless these societies have developed social conventions around concepts of privacy including knocking before entering, separate sleeping areas or psychological discretion. While there are no shared universal

conceptions, Solove believes that there are enough reoccurring similarities that can be pulled out and used to loosely frame the issues in a sensitive manner.³⁹

Sidestepping the assorted debates on the virtues, vices, intrinsic, instrumental or nonconsequentialist values of privacy, Solove argues in favour of a pragmatic value of privacy that is not universal but is situated in particular contexts. The value of privacy should be analyzed and balanced against competing social values. He asserts that the value of privacy should be understood and evaluated against its contributions to society. In other words, we protect individual privacy because it is good for society. Solove is careful to assert that privacy protects against a range of social problems, there is also a range of privacy values. He states that the general value of privacy arises out of the activities that it protects. "Privacy, therefore, is a set of protections from a plurality of problems..."⁴⁰

Taxonomy of Privacy Problems

Solove has created a specific taxonomy, or principles of classification, to describe the broad range of privacy problems. Solove recognizes that the value of a common language allows stakeholders to bring order to the discussion and solutions.

His taxonomy focuses on the specific activities that can and do create privacy problems.

³⁹ *Ibid.* at 76.

⁴⁰ *Ibid.* at 100.

Using Solove's approach, understanding the nature of the specific privacy problem allows stakeholders to work through the particular cultural variations and context and develop appropriate solutions. According to Solove, "The taxonomy aims to carve up the landscape in a way that the law can begin to comprehend and engage. All taxonomies are generalizations based upon a certain focus, and they are valuable only so far as they are useful for a particular purpose."⁴¹ Solove developed his taxonomy to assist the development of law and policy.

Generally, the taxonomy focuses on four groups of harmful activities each with associated subgroups of harms. The activities loosely follow the information flow. Beginning with the data subject, information is collected, processed, and disseminated. Each step results in consequences for the data subject.

⁴¹ *Ibid.* at 102.

Chart 1 – Model of Taxonomy⁴²

There are four ways Solove identifies privacy problems.

Solove is focused on the activities that create problems for the individual, or data subject. He identifies different types of privacy problems that emerge in the three different contexts that touch the data: information collection, information processing and information dissemination. He also identifies the problems that result in an impact, or invasion, on the data subject. During the information collection phase, the problem of surveillance arises when personal information is collected without the knowledge of the individual. Surveillance is viewed as problematic because it makes people feel psychologically uncomfortable, leading them to alter their normal behaviour or to self-censorship. Solove notes that surveillance could compromise social ideals and democracy

⁴² *Ibid.* at 104.

by inhibiting freedom of speech, open democratic participation, or expressions of creativity and self-development.

Once information has been collected, there are several problems associated with its processing. Processing involves the ways in which data is connected, transferred, linked or consolidated with other data. The reality of the modern information economy is that there are billions of dollars associated with the processing, analysis and reselling of personal information. Secondary use is one of the problems associated with information processing. Solove defines secondary use as “the use of data for purposes unrelated to the purposes for which it was initially collected without the data subject’s consent.”⁴³ This practice is problematic because there is a betrayal of the data subjects’ expectations or desires. Fears about secondary use lead to individual psychological concerns, distress or uncertainty. Secondary use can potentially cause real harm to the individual including denial of benefits or credit. There is also the possibility that data provided in one context may not be accurate in another leading to erroneous profiles, decisions or assumptions. The argument is often made that secondary use is problematic due to the deception involved and that an individual would not have released the information in the first place had they known it would be used in other contexts. The secondary use of personal information is often unknown to the individual and occurs beyond their ability of the individual to control.

Moving along the data continuum, after information processing there follows information dissemination. The broad activities associated with information dissemination also

⁴³ *Ibid.* at 131.

generate numerous privacy problems including breach of confidence, disclosure and increased accessibility. Information dissemination involves the circulation, revelation or threat of spreading information. Solove notes there are specific problems associated with the increased accessibility of personal information. There has always been personal information or official records available and accessible to the public. However, the realistic scope of what others could access about you was limited to small social or geographic areas.

In primitive society, an individual could only expect to be embarrassed by their family or immediate tribe. Today, the internet exponentially expands the potential for humiliation or violation. There is no proportionality of collection to information dissemination. Viral videos such as those of the Numa Numa Boy, Star Wars kid or Brittany Spears defender circulated beyond the initial social network to the whole world almost instantaneously without the individual's ability to restrict access or remove the material.⁴⁴ A public document available at a local courthouse could now be published to the world over the internet. While the information is already in the public or has been disclosed, the difference is one of quality and the exponential increase in risks of harm of disclosure. Some US courts are starting to recognize that there is a substantial or material difference between public records found through physical access to a courthouse and a digital, searchable, and openly accessible profile. Thus, there is a specific privacy harm of increased accessibility.⁴⁵

⁴⁴ "5 Most Viral Video Youtube Collection Watch Online" (5 April 2009), online: <<http://current-news-results-notice.blogspot.com/2009/04/5-most-viral-video-youtube-collection.html>>.

⁴⁵ Solove, *supra* note 19 at 151.

Soloves' final group of privacy problems illustrate the invasions that affect the individual. These privacy problems don't necessarily involve the specific bits of personal information initially collected, processed or disseminated but rather are the impacts or effects of the personal information eco-system, economy or infrastructure. A primary problem is that of intrusion or the invasion into a person's life that makes them feel violated, interrupts their solitude or causes disruption. Intrusion can be of an indirect manner such as unwanted photography or questioning or a physical intrusion such as receiving junk mail. Intrusion is problematic because it can prevent people from being able to retreat or seclude themselves from the presence of another. Desiring seclusion or places of sanctuary are both physically and psychologically important to human well-being.

Soloves' approach is helpful because once a privacy problem is clearly identified and understood, appropriate legal solutions can then be put forward. Further, the taxonomy allows for the potential of further work integrating the taxonomy with technology standards, design and development. This taxonomy could assist in the translation of legal policy into technical requirements. This will be discussed in more detail during the discussion of the DNCL policy in Canada in chapter 4. Soloves' work is new and has not yet been tested or implemented in a large scale by privacy practitioners. There is the possibility that fracturing privacy into minute quantifiable issues moves discussions away from a wholistic theory. There is also the potential that focusing on a pragmatic taxonomy based approach will diminish discussions of privacy as a civil or human right.

While Solove does incorporate a general sense of privacy as a social value, care must be taken not to lose sight of this when operationalizing a taxonomy based set of solutions.

Solove's taxonomy of privacy provides specific insights into the collection, use and disclosure of personal information by commercial organizations. His framework for identifying and understanding privacy problems provides a useful structure for courts, legislators and policy makers. Understanding the nature of the specific privacy threats and the rationale for protecting against them will assist in the development of more informed tools and decisions. By breaking out of the theoretical quagmire, effective responses to privacy can be envisioned. We will continue the discussion of the application of Solove's taxonomy of privacy problems during our examination of telemarketing in chapter four. In the next chapter, we will consider the impact of the current governance approach on the protection of personal information.

Chapter Three: Maturing a Privacy Governance System

“Privacy management is an old art form but a young science.”⁴⁶

In chapter two we discussed the ways in which Soloves’ taxonomy may help us define privacy problems related to the commercial collection, use and disclosure of personal information but there remains the related issue of effectively developing privacy solutions. An appropriate governance approach cannot be applied until there is recognition of the unhelpful assumptions that have underpinned traditional governance approaches (e.g., legislation). This chapter will start with a discussion of the limitations of this traditional governance approach as identified by Kernaghan Webb. This chapter will then consider evidence to illustrate three faulty assumptions that are undermining the protection of privacy in the traditional approach. First, it is generally assumed that business will respond to a consumer need. Secondly, it is believed that individuals can and will act in their own best interests. Finally, many people turn to the government to provide a legal solution. This section will demonstrate that businesses have not effectively responded to meet consumer privacy needs, that individuals either cannot or will not always appropriately advocate for themselves in their own best interest and that legislation has not been able to solve privacy problems in an appropriate or timely fashion. Each of these faulty assumptions undermines the foundation of an effective privacy solution and must therefore be dispelled before a more robust sustainable governance framework can be developed. This chapter will close with a discussion of

⁴⁶ International Security, Trust & Privacy Alliance, “Privacy Framework” Version 1.1 (2002), online: <<http://www.istpa.org/pdfs/ISTPAPrivacyFrameworkV1.1.pdf>>.

Kernaghan Webbs' framework for defining an inclusive, process based solution model: sustainable governance. The strengths of this model will be illustrated.

Governance is traditionally defined as “the sum of the many ways individuals and institutions, public and private, manage their common affairs.”⁴⁷ Governance can be analyzed and applied in a range of levels from the microanalysis of self or family governance to corporate and international governance. In this work, the term privacy governance is used to signify the broad range of political, legal, technological, economic, social and cultural instruments and processes that shape and in turn are shaped by the behaviour of actors and institutions. The concept of privacy governance thus refers to the various elements through which business, technology choices, governmental, social and individual actions are ordered and regulated. It includes a broad range of formal and informal actions including law creation, institution-building, process development, standards, self-governance, monitoring and enforcement. But it also includes a softer but no less important infrastructure of culture, norms, expectations, and social understanding of acceptable behaviour around privacy problems, in processes that engage the participation of a broad range of stakeholders.

In his chapter “Sustainable Governance in the 21 Century: Moving Beyond Instrument Choice”, Kernaghan Webb offers a compelling argument against exclusive reliance on conventional legislative or regulatory approaches and in favour of a broader, inclusive and informed use of the full range of actors, institutions, institutions and processes

⁴⁷ Commission on Global Governance, *Our Global Neighbourhood* (Oxford: Oxford University Press, 1995).

impacted by a social issue.⁴⁸ Webb asserts that a governance system that acknowledges and reflects the realities of governing in the 21st century, including the competing demands and budgetary limitations imposed on governments, will stand a better chance of being effective over the long term.⁴⁹ He calls this new type of governance system sustainable governance.

Webb provides a number of examples where governments have failed to adequately address important policy issues. He points to catastrophic failures of the state including the Walkerton water crisis or the collapse of the East Coast fisheries as examples of modern public-policy breakdowns. Typical responses to such events are public calls for more government money and resources invested as well as increased oversight and regulation. These demands from the public compete with business demands for less regulatory burdens and fewer taxes. In addition to meeting conflicting demands, governments must juggle jurisdictional conflicts, volatile economies, decreases in public trust and an increase of technological innovation creating new issues and exacerbating existing issues. The process of governing has grown much more complex in the last 50 years requiring a new vision that will allow for success in suboptimal conditions.

According to Webb, traditional government command and control regulatory instruments often form the foundation of a governance system. He illustrates the traditional

⁴⁸ Kernaghan Webb, "Sustainable Governance in the Twenty-First Century: Moving Beyond Instrument Choice" in Pearl Eliadia, ed., *Designing Government From Instruments to Governance* (Montreal: McGill-Queen's University Press, 2005) at 264.

⁴⁹ The general failure of the current governance assumptions with regard to privacy will be illustrated in this chapter and specific failure of the current approach will be outlined in detail in chapter four during the examination of the DNCL. Chapter five will apply some of Webb's conceptions to the DNCL in the effort to envision a next generation solution.

governance approach in chart form, reproduced below. In Webb's chart, governments are represented in the central arrow. However, in many instances industry has taken the initiative to develop instruments, institutions and processes that further the objectives of the command and control legislation through other means. In effect Webb's approach calls for recognition of the potential governance roles of entities other than government. This is particularly true in emerging technologies. However, in a sustainable governance approach if there is a downturn in the economy, or a shift in politics or resources that affect one sector, the other actors, institutions, instruments and processes can contribute by compensating, supporting or supplementing activities.

Diagram 2 – Sustainable Governance: Consumer Protection in Canada⁵⁰

The difficulties of governance are particularly relevant for consumer privacy. The weaknesses of a governance approach that relies too extensively on the capabilities, instruments, institutions and process of only sector of society are particularly evident when considering traditional approaches to privacy problems in Canada. In the sections below, we will consider the limitations of the traditional approaches to privacy protection. In particular, we will examine the protection of personal information that has relied respectively, on business, government or individuals, without sufficient

⁵⁰ Webb, *supra* note 48 at 264.

cooperation or coordination between all three actors or understanding their particular limitations.

Evidence of Immature Privacy Governance System

Business and Information Protection Technology

As collectors, users and distributors of consumer data, businesses are in a good position to be guardians of personal information and have strong incentives and motivations to do so, whether or not required by law. One of the purported strengths of a liberal capitalist economy is the ability of business to respond to and benefit from changing social, creative, political and economic situations. With few bureaucratic constraints, businesses can innovate quickly and freely to profit from new opportunities. Society can benefit from the introduction of goods, information and services to meet their needs and desires.

“Information is the lifeblood of the twenty-first economy.”⁵¹ And the information-based economy of modern western capitalist societies has been enabled by the information, communication and technology (ICT) revolution. Beginning with the development of the database in the 1940’s, to the emergence of desktop computing, through to the internet boom in the 1990’s, businesses have come to rely on technology an important tool. Businesses have used technologies to manage their traditional internal activities, to manage customer relationships, facilitate sales and marketing, as well as harness the

⁵¹ Fred Cate, *Privacy in Perspective* (Washington DC: The AEI Press, 2001) at 10.

explosive potential of ICTs to create entire new lines of business. Hardware installations of databases, computers, and fiber optics link offices and workers in exponential ways. Word processing, spreadsheets, data mining, and financial analysis software were all first developed for the business market. Technology has enabled business of all sizes and flavours to flourish. While the internet was not initially positioned as a commercial freeway, many businesses immediately adopted the technology and ran with it, developing e-shopping, corporate websites and direct, instantaneous and cheap-to-consumer advertising programs delivered through electronic mail, otherwise known as spam. The latest developments and uses for Radio Frequency Identification (RFID), wireless and nanotechnologies are still emerging. When a business opportunity or need has arisen, a technological solution has usually been quickly created.

As commercial organizations began to routinely collect, analyze and disseminate the ever growing pools of sensitive personal information as a part of their commercial activities, they also began to run huge reputational and financial risks if they misused or lost personal information. Businesses are now finding themselves increasingly subject to multi-million dollar class action lawsuits that could potentially destroy profitability and brand. The successful ChoicePoint class action law is one notable example.⁵² For the same reason, some businesses are highly motivated to champion the development and implementation of business policies and technological solutions to emerging privacy concerns. Several industry-championed privacy initiatives including initiatives sponsored by the Canadian Standards Association and the Better Business Bureau have

⁵² Dan Christensen, "Major Information Brokers Face Class Action for Invasion of Privacy" *LAW.COM* (24 June 2003), online: <<http://www.law.com/jsp/article.jsp?id=1056139884864>>.

demonstrated leadership and corporate social responsibility for their members. Some corporations, such as behavioural marketing company TruEffect, that understand the value of their information assets are developing privacy policies and turning to privacy enhancing technologies as a way of ensuring that they do not wrongly use or disclose information in violation of legislation or established industry best business practices.⁵³

However, because businesses can also gain competitive advantages from the sale, use and purchase of personal information, they also have incentives that can come into conflict with strong protections of personal information. Some businesses realized early on that information was a source of easy money and many set out deliberately to generate as much information seeding and harvesting as possible regardless of privacy and information best practices. As such, a major internal conflict of interest can be seen between business goals and privacy protection. Most of the information communication technologies themselves were not built with privacy or security in mind. Quite the contrary, the internet was designed to facilitate the collection and sharing of information accompanied by the computing power to process it.⁵⁴ The explosive growth of the ICT industry occurred in the absence of establishing robust privacy and security architectures, policies and deployments.

The ICT industry has grown and evolved in the last 20 years to provide wide-ranging sets of solutions in areas around communication, banking, and shopping. Technical innovations have led to heightened performance and increased efficiency. There is an

⁵³ TruEffect, online: <<http://www.trueffect.com>>.

⁵⁴ Federal Communications Commission, "Something to Share" (21 November 2005), online: <<http://www.fcc.gov/omd/history/internet/something2share.html>>.

active business and ICT industry that is potentially capable of generating and responding to robust consumer privacy best practices.⁵⁵ However, we can observe the systemic failure of the business and ICT communities to effectively impose protections for the personal information of consumers by observing the following factors:

1. The relative failure of a commercial Privacy Enhancing Technology (PET) and security technologies, architecture and infrastructures;
2. The increase in major privacy and data breaches;
3. The increase in identity theft;
4. The deployment of progressively more intrusive technology products.

A privacy enhancing technology (PET) is any technology that serves to eliminate the collection, use or disclosure of personal data, or gives direct control to the user over the revelation of their personal information. A privacy enhancing architecture or set of solutions refers to the whole system including all the different technologies, infrastructures, standards, protocols and processes used to protect privacy and personal information in data management and communications.

Currently, there are almost no accessible online anonymizing PET options available for the average consumer. Several PET projects were initiated but ultimately failed.

ZeroKnowledge, an anonymous communications company, collapsed in the internet bust in 2001. Critics at the time speculated that low subscriptions and a lack of viable business

⁵⁵ Government of Canada, "ICT and Canada: The Future Is Here", online: <<http://investincanada.gc.ca/eng/publications/ict-canada.aspx>>.

strategy were to blame.⁵⁶ Tor, an open source and somewhat ‘clunky’ anonymous communications product is also struggling for funding to commercialize its operations largely due to its inability to convince potential investors that there was a Return On Investment that justified its deployment. Anonymous e-cash product DigiCash also failed to institutionalize itself due to mismanagement and a reluctance of banks to take on an experimental product.⁵⁷ To date, there are no anonymous electronic consumer payment tools deployed in the market and there are no current plans to implement such tools.⁵⁸

Similarly, there are no ubiquitous privacy standards, architecture or protocols implemented for the internet or ICT infrastructures. The P3P (Platform for Privacy Preferences) initiative developed in 2002 was supposed to be the herald of user-centric, policy based privacy-conscious web browsers. However, seven years later, this initiative has failed to either go mainstream technologically or to gain traction with consumers.⁵⁹ While the International Standards Organization (ISO) has a smattering of isolated security standards, there has been insufficient progress to develop privacy technical or business standards and after many years nothing robust has emerged. The jumble of competing, conflicting and far too often weak technical standards, guidelines or best practice documents has contributed to the deployment of frail and isolated technical solutions. The effect of this lack of standards will be illustrated in the DNCL discussion in the next chapter.

⁵⁶ Felix Stalder, “The Voiding of Privacy” online: (August 2002) No.2 Sociological Research Online, <http://felix.openflows.com/html/FS_Voiding_of_privacy.pdf>.

⁵⁷ “How DigiCash Blew Everything”, *NEXT* (January 1999), online: <<http://jya.com/digicrash.htm>>.

⁵⁸ Quite the contrary, VISA plans to introduce RFID enabled credit cards.

⁵⁹ Roger Clark, “Business Cases for Privacy-Enhancing Technologies” in R. Subramanian, ed., *Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions* (Hershey, PA: IDEA Group, 2008), online: <<http://www.rogerclarke.com/EC/PETsBusCase.html>>.

Of course, there are numerous basic security tools and practices that can be implemented to minimize obvious security threats. However, in practice, an embarrassing number of companies are not using them. According to a 2007 Fusepoint Data Confidence Survey, one in five executives at Canadian companies report that their company currently does not use anti-virus software and one quarter of executives at Canadian companies report that their company operates without a firewall.⁶⁰ These findings are supported by a 2007 Litchfield study that found that half of the one million randomly tested online database servers were not protected by firewalls. Many of the servers with firewalls were out of date and unpatched for known vulnerabilities including the SQL slammer worm⁶¹ responsible for infecting over 22 000 systems worldwide within ten minutes in 2003.⁶² Symantec's Internet Security Threat Report reveals more than six million distinct bot-infected computers worldwide during the second half of 2006, representing a 29 % increase from the previous period. Trojans, computer code that performs a undisclosed malicious function, constituted 45 % of the top fifty malicious code samples, representing a 23% increase over the first six months of 2006. A zero-day vulnerability exists when a threat can exploit unknown or un-patched systems. There were twelve zero-day vulnerabilities documented during the second half of 2006, marking a significant increase from the one zero-day vulnerability documented in the first half of 2006. This data indicates that there is an increasing exposure of consumers and businesses to unknown

⁶⁰ Fusepoint News Release, "Fusepoint Data Confidence Survey" (24 October 2007), online: <http://www.fusepoint.com/english/downloads/FP_Survey_Release_Oct_07_ENG.pdf>.

⁶¹ Robert McMillan, "Half a million database servers 'have no firewall'" *IDG News Service* (14 November 2007), online: <<http://www.computerworlduk.com/management/security/data-control/news/index.cfm?newsid=6198>>.

⁶² David Moore, et al. "Inside the Slammer Worm" *IEEE Security and Privacy Magazine* (July/August 2003), online: <<http://www.cs.ucsd.edu/~savage/papers/IEEESP03.pdf>>.

threats, many of which could be prevented with known off-the-shelf protections or standard security protocols.⁶³

Equally disconcerting is a Gartner report in December 2006 that predicts that, by 2008, more than half of attacks against retailers will be directed at Point Of Sale systems and that by 2009, less than one-third of POS software will comply with prevailing already existing security standards.⁶⁴ An October 2007 Visa Inc. document stated that 35% of retailers are not complying with the payment card standards, which includes encryption standards.⁶⁵

Businesses have reported that they are overwhelmed by the technology and standards that have been deployed. Sharon Finney, information security administrator at DeKalb Medical Center in DeKalb County, Ga states: "I don't know of any business where employees have the time to read and comprehend every single policy related to a computer in their environment - they're busy doing their jobs."⁶⁶ Finney's statement illustrates a dominant sentiment that adhering to privacy and security standards is not a core component or priority of many businesses. These sentiments illustrate the failure of some businesses to self-regulate and validates a requirement for external regulation and

⁶³ Symantec, "Symantec Reports Rise in Data Theft, Data Leakage, and Targeted Attacks Leading to Hackers' Financial Gain" (19 March 2007), online:

<http://www.symantec.com/about/news/release/article.jsp?prid=20070319_01>.

⁶⁴ Robert L. Scheier, *supra* note 1.

⁶⁵ Visa, "PCI Compliance Continued to Grow in 2007", online:

<<http://www.corporate.visa.com/md/nr/press753.jsp>>.

⁶⁶ "The 8 most dangerous consumer technologies", *itWorldCanada* (6 September 2007), online: <<http://www.itworldcanada.com/a/The-good-the-bad-and-the-ugly/69d9da03-0842-4840-8526-1ba2a01b198e.html>>.

monitoring. Despite this, business self-government remains as an important component of a broader sustainable governance approach.

Despite all of the technical resources at their disposal, it appears that most businesses have not implemented universal, robust security protections for their ICT infrastructure, processes or equipment. The result, predictably, has been a notable increase in major privacy breaches.

Privacy Rights Clearinghouse has been keeping a list of major data breaches in the United States since the well-documented ChoicePoint breach in February 2005.⁶⁷

According to Privacy Rights Clearing house ,as of April 8, 2009, the number of US records containing sensitive personal information involved in security breaches was 253,753,738.⁶⁸ Since 2004, there has been a 1700% increase in data loss incidents.⁶⁹

The scope of the data records kept by single organizations also exacerbates the risk in a breach. The 2005 US CardSystems Solutions data breach affected as many as 40 million accounts affecting various credit-card brands.⁷⁰ In 2006 the U.S. Department of Veterans Affairs reported a loss of 26.5 million records pertaining to veterans and their families after a employee took a database home and it was stolen out of the house.⁷¹ In 2007, UK

⁶⁷“A Chronology of Data Breaches”, *Privacy Rights Clearinghouse* (April 2009), online: <<http://www.privacyrights.org/ar/ChronDataBreaches.htm>>.

⁶⁸ *Ibid.*

⁶⁹ Danielle Fournier, “Datagate - The 21st Century Scandal?” *Monitor Magazine*, online: <<http://www.monitortoday.com/Datagate.pdf>>.

⁷⁰ Robert Lemos, “MasterCard warns of massive credit-card breach”, *SecurityFocus* (17 June 2005), online: <<http://www.securityfocus.com/news/11219>>.

⁷¹ Robert Lemos, “Veterans Affairs warns of massive privacy breach”, *SecurityFocus* (22 May 2006), online: <<http://www.securityfocus.com/news/11393>>.

Revenue and Customs admitted to losing the details of 25 million individuals, with 7.25 million U.K. families potentially affected.⁷²

Most disturbingly, it appears that the problem of privacy breaches is much greater than is publicly reported. Former Information and Privacy Commissioner for the Province of British Columbia, David Flaherty, commented in the ETHI Identity Theft study meeting,

The problem I have is that a lot of the privacy breaches I'm aware of I have knowledge of under confidentiality agreements with my clients. I can't come and whistle-blow on my clients, but let me assure you, there are far more breaches taking place, which are far more sensitive in nature than you even read about in the newspaper. Hardly a week goes by that there isn't another privacy disaster that has happened.⁷³

It is understood that data breaches often lead to identity thefts. It stands to reason that an increase in data breaches will lead to an increase in identity theft. A recent Gartner survey indicates that 15 million Americans were victims of identity-theft related fraud in the twelve months ending in the middle of 2006, which is a 50% increase from 2003. The average loss per incident was \$3,257; more than twice the level for the same period in 2005 which indicates that there is not only more fraud, but the costs per victim is greater.⁷⁴ According to a Cyveillance survey phishing attacks, a fraudulent email sent to collect personal information, grew by 20% in the second quarter of 2007.

⁷² Tom Espiner, "U.K. government reveals its 'biggest privacy disaster'" *CNET News* (21 November 2007), online: <http://news.cnet.com/U.K.-government-reveals-its-biggest-privacy-disaster/2100-1029_3-6219772.html>.

⁷³ House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) Evidence, 39th Parliament, 2nd Session (8 May 2008) at 1650 (David Flaherty), online: <<http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=3484787&Language=E&Mode=1>>. ETHI is the Federal Sub-Committee responsible for privacy legislation.

⁷⁴ Robert L. Scheier, *supra* note 1.

While the business sector is struggling to protect personal information in existing ICT deployments, still new technologies are emerging to create new concerns. Microsoft has been championing CardSpace, an online single-identity service that consolidates and links all user registration and verification requirements in the name of user convenience. If not properly designed to protect privacy and anonymity, CardSpace, and other meta-identity solutions could result in establishment of mandatory authentication resulting in the eradication of functional privacy on the internet as we know it today. RFIDs embedded in item level goods including credit and debit cards could be used to track the physical location of individual consumers as well as profile their behaviour on a minute level.⁷⁵ Microsoft Health Vault is an online Personal Health Records that will allow for the collection, storage, and analysis of data and provide targeted ads based on the user uploaded data. RFIDs mean that a data collection company can go through your garbage, see what you bought, how long you used it and if you bought items from other jurisdictions.⁷⁶

The above examples demonstrate how the rapid expansion in the technology sector is tainted if the technology is not developed with a privacy architecture, appropriate security measures or required performance standards. It is evident that the technology sector has failed to self-generate and disseminate appropriate privacy technology solutions. The above examples also illustrate that the traditional free market approach has not generated

⁷⁵ Katherine Albrecht, "Supermarket Cards: The Tip of the Retail Surveillance Iceberg", online: (Summer 2002) Volume 79, Issue 4 Denver University Law Review, <<http://www.spsychips.com/documents/Albrecht-Denver-Law.pdf>>.

⁷⁶ *Ibid.* at 534.

privacy solutions to problems that already exist in current technologies, and that it is unlikely to decrease privacy concerns arising from emerging technologies.⁷⁷

There are several justifications that have been set out for the lack of privacy enhancing technologies in the marketplace. Some analysts point their fingers at the technology bust in the first half of the millennium drying up investment funds. Other corporate behaviours have indicated that there is simply little market demand or return on investment in privacy technologies.⁷⁸

Ross Anderson in his 2001 paper “Why Information Security Is Hard -- An Economic Perspective” articulated the fundamental reason for the failure to develop privacy enhancing solutions most clearly. According to Anderson, in our current environment, “the party who is in a position to protect a system is not the party who would suffer the results of a security failure.”⁷⁹ There is little motivation or profit for corporate leaders in a cost driven economy to require and enforce privacy standards. There has been a general failure to develop an economic rationale to counteract the belief that privacy costs money, rather than generates or at least saves it. Finally, in the post 9/11 context the financial investment in security (privacy invading) technology was both robust and

⁷⁷ In chapter four we will further discuss the role of technology development within a comprehensive privacy governance system.

⁷⁸ Computing in Medicine Research Group Memorial University of Newfoundland, “Private / Public Sharing of Personal Information: Lessons from the health care sector” Office of the Privacy Commissioner of Canada Contributions Program (March 2008) at 51.

⁷⁹ Ross Anderson, “Why Information Security Is Hard - An Economic Perspective” (Computer Security Applications Conference, 2001), online: <<http://www.cl.cam.ac.uk/~rja14/Papers/econ.pdf>>.

enthusiastic, reflecting and responding to the broader political climate that did not uphold privacy as a core value.⁸⁰

Although business weaknesses have been identified, appropriate business response to consumer issues is an important component of a sustainable governance approach. Business involvement is required and desired to utilize their particular expertise, capacity and resources. Traditionally, because of the failure of businesses to effectively self-regulate, there is a need to rely on some form of government response. The role of government has grown to balance competing social and economic interests and thereby protect the public. It will be demonstrated below that government responses, particularly legislation, also contain several practical limitations.

Government and Legislation

It is true that behavior cannot be legislated, and legislation cannot make you love me, but legislation can restrain you from lynching me, and I think that is kind of important. Martin Luther King⁸¹

Webb argues that conventional legislative and regulatory approaches have become increasingly limited in the face of modern governance issues. This is particularly true for the issue of privacy. In the modern international information era, jurisdictional constraints hinder governments' abilities to regulate or affect redress for citizens. Within borders, there are often limited incentives for regulated actors to undertake activity

⁸⁰ Tom Head, "Privacy After 9/11" *About.com*, online: <http://civilliberty.about.com/od/waronterror/ig/War-on-Terror-101/Privacy-After-9-11.htm>.

⁸¹ Cindy Leise, "When MLK came to Oberlin", *The Chronicle-Telegram* (21 January 2008), online: <http://www.chroniclet.com/2008/01/21/when-mlk-came-to-oberlin>.

beyond that required by prescribed minimal standards, this often results in a culture of mediocrity.⁸² The variable financial resources of the state coupled with pressures stemming from the international nature of the information economy and advances in ICT technology can result in an inability to oversee, investigate or enforce compliance. Further, governments experience difficulties in amending legislation or regulatory terms to address evolving problems in a timely and effective manner.⁸³

Many of these weaknesses can be observed in the Canadian context through an analysis of the effectiveness of *PIPEDA*. In response to increasing concerns about personal privacy in the information economy, the Canadian federal government passed the *Personal Information Protection and Electronic Documents Act (PIPEDA)* in 2001.⁸⁴ *PIPEDA* stipulates how private sector organizations may collect, use or disclose personal information in the course of commercial activities.⁸⁵

PIPEDA was constructed around a consumer consent model. For the most part, businesses must have the knowledge and consent of customers to collect, use or distribute their personal information. *PIPEDA* allows a consumer or their agent to contact a commercial organization that is subject to *PIPEDA* and notify that organization that the organization should not collect, use or disclose the consumer's personal information. An individual is also able to directly challenge the compliance of a commercial

⁸² The DNCL discussion in the next chapter will illustrate this point in more detail.

⁸³ Webb, *supra* note 48 at 245.

⁸⁴ *Personal Information Protection and Electronic Documents Act (PIPEDA)*, S.C. 2000, c. 5 [*PIPEDA*].

⁸⁵ The *Privacy Act*, R.S.C. 1985, c. P-21. is the legislation that governs the collection, use and disclosure or personal information by federal government departments and agencies.

organization.⁸⁶ An individual may file a complaint with the Office of the Privacy Commissioner of Canada and it is the role of the Privacy Commission of Canada to respond to such inquiries, initiate an investigation, mediate a solution and write a report of findings. The Office of the Privacy Commissioner also has the authority to initiate a court application. While not within the powers of the Office of the Privacy Commissioner, a court can order a company to correct its practices, publish the notice of action against an organization or award damages to the complainant.⁸⁷

This legislation applies to all federally regulated private sector companies and selected provincially regulated companies where provinces haven't adopted their own 'substantially similar' legislation. There is currently a patchwork of legislation in Canada as some provinces have instituted their own consumer and health privacy laws. Alberta, British Columbia, Ontario and Quebec have all had their provincial legislation declared in whole or in part to be substantially similar to *PIPEDA*.⁸⁸ Employee privacy protection has different considerations depending on the jurisdiction or sector.⁸⁹

While there is an articulated federal law and regulatory system in place, we can observe that the law and the legislative process that created and supported it are relatively weak by considering the following factors:

⁸⁶ *PIPEDA*, *supra* note 84, Schedule 1 - Principles.

⁸⁷ *Ibid.*, Division 2 - Remedies.

⁸⁸ Office of the Privacy Commissioner of Canada, "Substantially Similar Provincial Legislation", online: <http://www.privcom.gc.ca/legislation/02_06_01_e.asp>.

⁸⁹ Office of the Privacy Commissioner of Canada, "Privacy in the Workplace", online: <http://www.privcom.gc.ca/fs-fi/02_05_d_17_e.asp>.

1. Research indicates there is relatively low business compliance with even the most basic *PIPEDA* requirements;
2. The recent five year mandated *PIPEDA* review process illustrates the lack of timely responsiveness, overly political nature of the process and unequal representation of participants.

Compliance with PIPEDA

In 2006, Canadian Internet Policy and Public Interest Clinic (CIPPIC) conducted a research project to document Canadian business' compliance with *PIPEDA*.⁹⁰ CIPPIC found that there was widespread non-compliance in the four areas they evaluated.

- In violation of Principle 5 - Consent – one half to 2/3 of companies admitted that they shared information with third parties for purposes other than the transaction;
- In violation of Principle 8 – Openness – in 22% of the cases it took over ten minutes to answer basic privacy questions such as “Do you have a privacy policy?”, “How can I get it?”;
- In violation of Principle 8 – Openness – a significant proportion of privacy policies were deemed unclear;
 - 22% of policies were unclear about the purpose for collection;
 - 30% of policies were unclear about how the company use the information;

⁹⁰ Canadian Internet Policy and Public Interest Clinic (CIPPIC), “Compliance with Canadian Data Protection Laws: Are Retailers Measuring up?” (April 2006), online: [http://www.cippic.ca/documents/bulletins/compliance_report_06-07-06_\(color\)_\(cover-english\).pdf](http://www.cippic.ca/documents/bulletins/compliance_report_06-07-06_(color)_(cover-english).pdf).

- 45% of policies were unclear about whom the company disclosed information;
- In violation of Principle 8 – Openness – a high proportion of company policies were incomplete;
 - 30% of policies did not provide contact information for a privacy officer;
 - 38% of policies did not reference the individual’s right (per *PIPEDA*) to access their information;
 - 27% of policies did not describe the type of information held by the company;
 - 34% of companies that admitted to sharing information did not describe the type of information they shared;
 - 86% of companies that admitted to sharing information did not describe with whom they shared information with;
- In violation of Principle 9 - Individual Access - 25 out of 72 companies, representing 35 % of the companies tested, did not respond to the request to access to the personal information. Of the companies that did respond to the CIPPIC researcher’s request;
 - 42% failed to provide details about the Requestor’s personal information held on file;
 - 37% provided no or inadequate account of how they used the personal information;

- 58% did not give a list of companies to whom they have or may have disclosed personal information;⁹¹

A similar compliance study was also conducted by Marie Vallee through the French consumer group Option Consommateurs funded under the auspices of Industry Canada. While there were several key methodological differences between the studies, including the fact that the Option des Consommateurs study was much smaller, the parallel results are revealing.⁹² Vallee's study found:

- In violation of Principle 9 - Individual Access - three companies, representing 25 % of the twelve companies tested did not respond to the inquiries made;
- In violation of Principle 9 - Individual Access – only 22% provided the Requester with a full account of Personal Information;
- In violation of Principle 8 – Openness - no company provided the Requester with a list of companies with whom they had (or may have) shared the requester's information or to whom they may have disclosed the information;

The Office of the Privacy Commissioner commissioned EKOS Research Associates in early 2007 to undertake a comprehensive examination of public opinion and corporate privacy practices to establish a number of benchmark measures to help in the review of PIPEDA. According to the report, “the findings suggest there is a clear need to raise

⁹¹ *Ibid.* at iv & v.

⁹² Option Consommateurs, “Right of Access to Personal Information: The Key to the Right of Privacy” (2006), online: <<http://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca02075.html#projf>>

awareness of a company's responsibilities under Canada's privacy laws".⁹³ The findings of the report include:

- 31 % of Canadian businesses are either still in the process of complying with *PIPEDA* or have yet to begin;
- Only a third of all businesses report having staff that has been trained about the practices and responsibilities under Canada's privacy laws;
- In violation of Principle 9 - Individual Access – 20% of companies have not implemented any method in which consumers could attain access to their information;
- In violation of Principle 8 – Openness – 75% of businesses did not have a privacy policy posted online;⁹⁴

These results have been confirmed by the Office of the Privacy Commission itself.

According to a study commissioned by the OPC and conducted by IDC research group:

- 31% of businesses are either still in the process of complying with such law or have yet to begin;
- Less than 10 percent of medium-sized and large Canadian firms believe their lack of compliance with privacy legislation is a threat to them;⁹⁵

⁹³ Office of the Privacy Commissioner of Canada, "Canadian Businesses and Privacy-Related Issues" by EKOS Research Associates (March 2007), online:
<http://www.privcom.gc.ca/information/survey/2007/ekos_2007_01_e.asp#summary>.

⁹⁴ *Ibid.* at section 2.

This body of research indicates that there is widespread systemic poor compliance with even the most basic *PIPEDA* requirements. Results indicate that businesses know they have privacy and data protection responsibilities but on the whole fail to meet them. While some organizations may claim a lack of capacity and resources to meet complicated privacy obligations, the length and obscurity of other organizations privacy statements indicate a willful attempt to follow the letter but not the spirit of the privacy law.

The documentation of widespread lack of compliance has specific implications for the current enforcement regime as well as future changes to the enforcement regime. The Office of the Privacy Commissioner is responsible for overseeing compliance of *PIPEDA*. However, the Office is currently designed following a non-confrontational ombudsman model. The OPC does not have order-making powers and has limited abilities to proactively initiate a complaint, audit or disclose activities of an organization under investigation.⁹⁶ CIPPIC concludes in their report that the enforcement regime is the most important issue for Parliament to consider in the *PIPEDA* review process.⁹⁷ While a more robust enforcement regime would increase *PIPEDA*'s effectiveness, as we will discuss below, even a more effective legislative and regulatory response is not enough on its own to fully protect consumer privacy.'

⁹⁵ Shane Schick, "Canadian businesses stumbling over privacy compliance" *Computerworld* (25 July 2007), online:

<<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9027951>>.

⁹⁶ Office of the Privacy Commissioner of Canada, "Statutory Review of the Personal Information Protection and Electronic Documents Act Background Information on the OPC's Consultation" (27 November 2006), online: <http://www.privcom.gc.ca/parl/2006/sub_061127_e.asp>.

⁹⁷ CIPPIC, *supra* note 90 at 42.

PIPEDA Review Process

PIPEDA received royal assent in 2000 accompanied by a three year, three-stage implementation schedule, including a mandated review requirement. The five year mandated *PIPEDA* review process began in the fall of 2006. The *PIPEDA* review process illustrates weaknesses and challenges associated with legislative responses to social problems. The following general observations can be made about the process and its results:

1. The committee process was rushed and often sidelined due to political pressures of the day.
2. There was a minimal representation of civil society representatives in comparison to industry lobbyists resulting in a skewed representation of the situation.
3. Many committee members did not understand the issues – either the technology or the social dimensions.
4. The recommendations emerging out of the committee were minimal and did not resolve issues that have emerged with newer technologies.
5. It will take several years after the review to draft and implement any changes.

There are implications of each of the above observations.

The House of Commons Access to Information, Privacy and Ethics committee (known as ETHI) was responsible for overseeing the statutory *PIPEDA* review and is also

responsible for studying matters related access to information and government ethics. During the committee's regularly scheduled *PIPEDA* meeting times there were regular interruptions by committee members wishing to address other topics. Time and focus was continually redirected from the *PIPEDA* review to other political matters.⁹⁸ When the public consultation phase came to an end in the spring there was not much time left to complete the process during that sitting of Parliament, which was also threatening to be cut short by the potential fall of government. During a public speaking appearance during the writing of their report, committee chair Tom Wappel acknowledged that the committee review process and deliberation was rushed and pressed for time because they wanted to submit a report before the Conservative minority government fell or broke for summer.⁹⁹

The list of witnesses testifying before the committee also revealed unequal participation across the different sectors of society. There were twelve government and law enforcement representatives in total. Four of these were from federal departments providing background context, four were from the offices of the federal Privacy Commissioner offices and four were from law enforcement agencies asking for increased powers to overrule *PIPEDA* protections. In contrast, there were forty industry witnesses who either argued for the status quo (specifically against order making powers or naming of names), exemptions or clarifications for their industry. The one exception was Joseph Bozic from the National Association for Information Destruction who wanted specific

⁹⁸ House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) Evidence, 39th Parliament, 1st Session (4 December 2006) Carole Lavalley at 1705, online: <http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=2564268&Language=E&Mode=1&Parl=39&Ses=1>.

⁹⁹ Tom Wappel, "Oral Comments" (CPO Roundtable, 6 March 2007).

destruction guidelines articulated.¹⁰⁰ There were eight privacy / consumer advocates or academics and two representatives of Canadian Resource Centre for Victims of Crime, Steve Sullivan and Krista Gray-Donald, who advocated for more powers for law enforcement agencies.¹⁰¹ As compared to the corporate sector representation, there was only minimal representation of civil society groups and the lack of a robust civil society representation arguable resulted in a skewed representation of the relevant concerns with the legislation before the committee. There was a little to no discussion of the consideration of increased privacy protection from a human rights perspective.

It was evident during the *PIPEDA* review process that ETHI committee members, who are all elected officials, did not have a thorough understanding of the issues. On November 29, 2006, children's privacy expert Dr. Val Steeves appeared before ETHI and illustrated several current privacy issues associated with children's online websites. She also demonstrated how current technology could foreseeably be extended to invade privacy. MP Carolle Lavalee questioned Dr. Val Steeves on the perils of privacy invading technology.

I was very surprised by your presentation which was bordering on science-fiction. I could hardly believe the examples you gave us Even if it were possible to do it, I think it would be economically unrealistic because of the high cost of technology. It would also be technically quite difficult¹⁰²

¹⁰⁰ Although self-serving for the benefit of their members, I believe this requirement would make sense for heightened consumer protection. Alas, this recommendation was rejected.

¹⁰¹ Canadian Resource Centre for Victims of Crime, "Brief to the Standing Committee on Access to Information, Privacy and Ethics Re: PIPEDA Review" (13 February 2007), online: <<http://www.crcvc.ca/docs/PIPEDA.BRIEF.pdf>>.

¹⁰² House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) Evidence, 39th Parliament, 1st Session (29 November 2006) Carolle Lavalee at 1605, online: <<http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=2555892&Language=E&Mode=1&Parl=39&Ses=1>>.

On February 1st after ten days of hearings and two thirds of the way through the process, conservative MP and vice-chair of the review committee David Tilson commented,

I'm obviously on mailing lists. I don't know how they get my name and address...and What happens? How did we get on those mailing lists?"¹⁰³

Conservative MP Mike Wallace stated for the record,

"I'll be frank. I was involved in municipal council for 13 years, active in business for 20-some years since graduating from university, and since I've been here, it's the first time I've heard of [PIPEDA]."¹⁰⁴

These comments are problematic because they demonstrate how many of the politicians involved don't understand the problems associated with currently deployed information and communication technologies such as online information collection and telemarketing and therefore have little ability to understand emerging technology issues such as biometrics and RFIDs. This fundamental disconnect will result in legislation and policy that is already out of date.

In their presentation to the committee, CIPPIC made several specific recommendations.

In particular, CIPPIC recommended that the legislation should be amended to include:

- Commission order making powers;
- Mandated naming names of companies found in violation;
- Class action suits against companies believed to be in violation;

¹⁰³ *Ibid.* (1 February 2006) David Tilson at 0955, online: <<http://cmte.parl.gc.ca/cmte/CommitteePublication.aspx?SourceId=191464&Lang=1&PARLSES=391&JNT=0&COM=10473>>.

¹⁰⁴ *Ibid.* (6 December 2006) Mike Wallace at 1640, online: <<http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=2583398&Language=E&Mode=1&Parl=39&Ses=1>>.

- Removal of financial disincentives to pursue action / assistance to make a claim at the federal level;
- Punitive damages against companies found to be in violation;
- Allowances for spot audits of companies by the commissioner ;
- Mandated reporting of breach statistics to commissioner;

In the Committee's final report, each of these recommendations was subsequently rejected by the committee. ETHI's wholesale rejection of most of the recommendations that provided additional consumer protection and legal redress indicates a failure of the Committee to take the opportunity to reposition *PIPEDA* as a consumer protection tool.¹⁰⁵

While ETHI rejected civil society recommendations, the Committee adopted the IMS definition of work product despite the Privacy Commissioners' reluctance to address the issue.¹⁰⁶ Similarly, following the recommendation of Information Technology Association of Canada the Committee recommended that no amendments should be made to restrict transborder flows of Canadian personal information.¹⁰⁷ In their formal report, the ETHI committee agreed to study issues of breach notification, children's privacy as well as to clarify what is meant by "government institutions" in s.7 (3). While the committee agreed to clarify the consent requirements and repeal the *Public Safety Act*

¹⁰⁵ House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) "Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics" 39th Parliament, 1st Session (May 2006), online: <http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=2891060&Language=E&Mode=1&Parl=39&Ses=1&File=5>.

¹⁰⁶ *Ibid.* Recommendation 2.

¹⁰⁷ *Ibid.* Recommendation 16.

amendment (collection for law enforcement purposes without consent) this was rejected by the government response to the committee report.¹⁰⁸

The results of the *PIPEDA* review process and ETHI's recommendations indicate that there will be no substantive repositioning or reconceptualization of *PIPEDA* as a consumer protection instrument. For the most part, the process followed the lead and recommendations of industry.

Despite the minimal or tepid innovation in *PIPEDA*, even in a best-case scenario it will be several years before the law can be amended, passed through Parliament and receive assent. The process is slow due to parliamentary committee procedure and a general lack of political will to expedite. The former Deputy President of the Netherlands Data Protection Authority, Dr John Borking has noted that "technological change is 30 times faster than the speed that the law can be changed: PC product lifetimes are about 9-24 months, Internet product lifetimes are about 4-7 months while law making can take 7-12 years."¹⁰⁹ The protracted and expensive legislation development and implementation processes themselves illustrate the relative difficulty of governments to respond to complex issues of national and international information protection in the internet age.¹¹⁰

¹⁰⁸ Government of Canada, "Government Response to the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics: Statutory Review of the Personal Information Protection and Electronic Documents Act" 39th Parliament, 1st Session (2006), online: <http://www2.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&Parl=39&Ses=1&DocId=3077726&File=0>.

¹⁰⁹ Dr John Borking, Oral remarks at the 21st International Conference on Privacy and Personal Data Protection, Hong Kong, China (September 1999).

¹¹⁰ Kernaghan Webb "Government, Private Regulation, and the Role of the Market," in Michael MacNeil et al, eds., *Law Regulation and Governance* (Toronto: Oxford University Press, 2002) at 240.

There are several justifications that can and have been made for the failures of the legislative response to privacy concerns. The primary rationale is that *PIPEDA* is just in its early days and that business needs time to adjust.¹¹¹ A secondary rationale is the lack of available resources for enforcement. The Federal Privacy Commissioner stated in the ETHI committee session that she felt the powers the office currently possesses were sufficient and had expressed concern for taking on additional enforcement activities due to a lack of resources.¹¹² A third factor is that at the time of the *PIPEDA* review there was a Conservative minority government in power that was dealing with criticisms about the participation in the war in Afghanistan and the political reality was that privacy and data protection was not a priority.

The counter argument can be made that the Canadian Standards Association Privacy Code has been in place since 1996 and businesses have had almost ten years to adjust if they were so motivated. *PIPEDA* had been available for five years for businesses to review and adopt at any time prior to the mandated compliance date. Another reality is that while the Commissioner has the power to publish the names of offenders, the office has only done so on two occasions. In 2003, shortly after the current Commissioner's appointment to her office the Public Interest Advocacy Centre called upon her to name names in her findings.¹¹³ Her response was to study the issue but to date there has been

¹¹¹ House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) "Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics", *supra* note 109, at 1.

¹¹² House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) Evidence, 39th Parliament, 1st Session (22 February 2006) Jennifer Stoddart at 0910, online: <<http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=2735086&Language=E&Mode=1&Parl=39&Ses=1>>.

¹¹³ Public Interest Advocacy Centre, "Letter to Privacy Commissioner of Canada" (18 December 2003), online: <http://www.piac.ca/privacy/letter_to_privacy_commissioner_of_canada_1/>.

no publication of her findings.¹¹⁴ Clearly, there is little will by the commissioner to step out of an ombudsman role. Ultimately, while the current legislation is a central part of the solution, it is not sufficient on its own.

The above examples demonstrate the considerable challenges associated with full and effective implementation of legislation regulating private or corporate behaviour especially if the legislation is out of date, weak or incomplete. The introduction of legislation does not guarantee a change in behaviour or ensure compliance with that law. The above examples also illustrate that the traditional government legislative process has not resolved the privacy problems it has already undertaken to address let alone the issues arising from emerging technologies such as biometrics or RFIDs. In chapter five we will further discuss the role of government and law within a comprehensive sustainable privacy governance system.

Lacking the expertise and resources of both the corporate and government sectors, it can be claimed that the actor most vulnerable to privacy invasions is the individual. The current privacy legislation is supposed to protect the individual. However, the traditional liberal argument within our capitalist system relies on the assumption that individual are responsible for acting in their own self interest. This mistaken belief is discussed below. While the individual is the victim when their personal information is misused, it can also be argued that they contribute to the problem.

¹¹⁴ Office of the Privacy Commissioner of Canada, "Privacy Commissioner Response to PIAC Proposal" (12 January 2004), online: http://www.piac.ca/privacy/privacy_commissioner_response_to_piac_proposal.

The Individual and Individual Capacity

The individual person and their personal data are at the epicentre of our current privacy protection regime. Individuals positioned at the centre of the information flow are in a pivotal position to protect and control information about themselves. They are the source of personal information and those who are most affected by intrusion into their private lives. Individuals have the strongest motivation for not disclosing their information without purpose and to be watchful over their information once disclosed. It is the individual who ultimately suffers the social humiliation when their sensitive information is disclosed or pays a financial cost when their credit is compromised. Within the liberal tradition, the individual is expected to be empowered to use the tools available to advocate on their own behalf.

In our Western liberal tradition, individuals are accorded the right and responsibility to govern their own affairs. *PIPEDA*, and most of western privacy legislation, was built on the foundations of rational self-interest and informed consent. Under *PIPEDA*, businesses have the responsibility to get consent before collecting or using the personal information they are soliciting.¹¹⁵ There is an assumption that individuals will assess the request for personal information collection and will grant or refuse consent based on self-interest.

However, the capacities of individuals to make effective decisions as well as the constraints within which individuals are forced to operate serve to weaken the

¹¹⁵ *PIPEDA*, *supra* note 84, Principle 3 - Consent 4.3.1.

effectiveness of this doctrine. In fact, the assumption that individuals are empowered to make appropriate choices about the disclosure and use of their personal information is undermining the evolution of privacy protection. In practice, the evidence illustrates that individuals are not as watchful over their disclosure of personal information as rationality would dictate. Research into consumer behaviour, psychological economics and bounded rationality theory illustrate that individuals routinely do a poor job about making rational decisions. Business practices depend on this unconscious consumer compliancy in order to push the envelope of data collection. This is further complicated by the relative inability of the individual to recollect or safeguard their information once it has passed from their control into the corporate realm or expanse of the information universe.

While there is an ingrained assumption that individuals have the ultimate power over their privacy decisions, we can observe that this assumption is flawed for at least the following reasons:

1. People don't choose the most privacy;
2. Consumers lack ability and tools to make effective privacy decisions;
3. Individuals lose the ability to control the information once it flows.

People don't choose the most privacy

As noted above, consent is the foundation upon which government legislation, such as *PIPEDA* is premised. Consent is also the foundation of commercial approaches to personal information. For example, Microsoft's user-centric system architecture, as

defined in their Laws of Identity, sets individuals at the centre of the model to make decisions over the release of their personal information. If individuals consent to release information, anyone can collect it.¹¹⁶

The limits of consent as a barrier to misuse of personal information have been well documented. There are numerous examples where individuals have been demonstrated to be willing and / or enticed to give up extremely personal and sensitive information for essentially modern trinkets and beads such as a chance at travel, fifty-cent coupons or personalized emails for upcoming sales. Loyalty programs and consumer survey panels are the best examples, as they exist almost exclusively to gain more and specific information on consumers. The largest Loyalty Program in Canada is the Air Miles program. This program has almost 10,000 business partners with whom it shares personal information for a price. Personal information collected includes biographic information, shopping patterns and financial data. This information is then used for marketing purposes. Loyalty programs continue to grow in membership, from fewer than 40 percent of the general population in 1993 to 67 percent in 2003¹¹⁷ even as organizations such as Aeroplan became subject of an OPC decision in 2002.¹¹⁸

In a recent social engineering experiment, researchers in England stood on the street and gave out chocolate bars in exchange for personal information including names, phone

¹¹⁶ Kim Cameron, "Introduction to the Laws of Identity" *Kim Cameron's Weblog* (8 January 2006), online: <<http://www.identityblog.com/?p=354>>.

¹¹⁷ Canada, Office of Consumer Affairs, "Consumer Trends Report" (20 September 2007), online: <<http://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca02096.html#tlc>>.

¹¹⁸ Office of the Privacy Commissioner of Canada, "Letter to Air Canada's Manager of Privacy Compliance, Erik Grados" *News Release* (20 March 2002), online: <http://www.privcom.gc.ca/media/nr-c/02_05_b_020320_e.asp>.

numbers and passwords from passers-by.¹¹⁹ A recent behavioural economics experiment indicated that privacy decisions are highly contextual and influenced by the medium. Contrary to logic, people were more likely to respond more fully to an informal online questionnaire with no assurances of confidentiality than a professional website with a clear indication of confidentiality.¹²⁰ These studies tell us that consumers can be enticed to reveal personal information fairly easily.

Consumer behaviour literature also indicates that consumer behaviour is not rational in the strict sense. In a recent study, the Ponemon Institute reported that only 31% of respondents cut ties with an organization after a data breach. While its findings are worthy of further investigation, this report indicates that breaking ties with a business takes time and effort and many consumers are willing to put up with poor business practices rather than go through the hassle of switching.¹²¹

Consumers lack capacity and tools to make effective privacy decisions

The ability of individuals to give consent requires an understanding that they have the capacity to consent. The ability of individuals to act in their own best interest is also affected by the conditions under which consumers are forced to make decisions. In CIPPIC's *PIPEDA* compliance study discussed above, researchers found the vast majority of the privacy policies were long (63% over 1000 words) and written in such a

¹¹⁹ Steve Ragan, "Company privacy traded for candy" *The Tech Herald* (17 April 2008), online: < <http://www.thetechherald.com/article.php/200816/737/Company-privacy-traded-for-candy/>>.

¹²⁰ Brad Stone, "Our Paradoxical Attitudes Toward Privacy" *The New York Times* (2 July 2008), online: <<http://bits.blogs.nytimes.com/2008/07/02/our-paradoxical-attitudes-towards-privacy/?th&emc=th>>.

¹²¹ Ponemon Institute, "Consumers' Report Card on Data Breach Notification" (15 April 2008).

way that they are beyond the scope of the average person to understand according to standard readability tests, and indeed beyond the comprehension of several of the researchers themselves. Most disturbing was that 18% of policies offered misleading information that the company offered opt-in consent when in fact they really used opt-out consent models leaving individuals to assume that they were protected when they were not.¹²²

Similarly, a recent Carnegie Mellon study revealed that the average corporate privacy policy would take ten minutes to read. The study was based on the privacy policies used by the 75 most popular US websites and found that the average length of privacy policies were 2,500 words which translates roughly into five pages.¹²³ While there has been some work done on ways to make privacy policies more accessible, the Carnegie Mellon study indicates that few organizations have actually implemented them.¹²⁴

Many of the current identity theft strategies articulated by government, business and consumer organizations suggest that consumer education and responsible data practices can assist in preventing identity theft. These practices include using a personal shredder for paper documents, not giving out personal information over the phone, protecting your computer by using a firewall, anti-virus software, and being wary of any attachment or

¹²² CIPPIC, *supra* note 90 at i.

¹²³ Aleecia McDonald and Lorrie Faith Cranor, "The Cost of Reading Privacy Policies" (Paper Presented to the Telecommunications Policy Research Conference, 26 September 2008), online: <<http://www.scribd.com/doc/7550344/Cost-of-Reading-Privacy-Policies>>.

¹²⁴ Corporate Solutions Consulting, "Fair Processing Notifications: Current Effectiveness and Opportunities for Improvement" (22 January 2007), online: <http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/ic_final_report_version_1.1_final.pdf>.

download from emails you receive, regardless of who sent them.¹²⁵ While these are reasonable and responsible practices, as we observed above, they are not where the individual is most vulnerable to a loss of personal information.

The Federal Privacy Commissioner, Jennifer Stoddart, noted in a 2006 speech to the Canadian Marketing Association's Regulatory Affairs conference that loyalty programs are not often transparent with consumers about the 'real' information collection, use and disclosure practices and the underlying profit motivations driving organizations.¹²⁶ The average consumer does not fully understand, therefore is incapable of consenting to, or protecting themselves from, the barrage of technical and marketing requests for personal information. A recent study revealed that the percentage of victims who knew how their data was lost actually fell from 6% to 3% from 2005 to 2006.¹²⁷ A Canadian study reported that 28% of respondents indicated they did not know how to protect themselves or know enough about ID theft.¹²⁸

Interestingly, research out of Australia reports that an individual's level of concerns around privacy and his or her willingness to trade personal information for cheaper prices was largely dependent on their education and socio-economic status. Their findings

¹²⁵ Public Safety Canada, "Advice for Consumers Identity theft" (03 May 2008), online: <<http://www.publicsafety.gc.ca/prg/le/bs/consumers-en.asp>>.

¹²⁶ Office of the Privacy Commissioner of Canada, "Privacy in the Marketplace Remarks for CMA Regulatory Affairs Conference" (Public Address by Jennifer Stoddart, 14 September 2006), online: <http://www.privcom.gc.ca/speech/2006/sp-d_060914_e.asp>.

¹²⁷ Robert L. Scheier, *supra* note 1.

¹²⁸ Sigma Assistel, "Cross-Canada survey on Identity Theft" (13 June 2007), online: <<http://www.assistel.com/NR/rdonlyres/0DA419C3-156E-4EEE-93C6-3902C3A0FD48/0/PressRelease.pdf>>.

reveal that wealthier and better-educated people with an understanding of the issues are able to make informed judgements and active choices about the individual's privacy while people with lower levels of education and understanding of the issues have less capacity to actively protect their privacy.¹²⁹

Consumers lose the ability to control the information once it flows

Regardless of how or why the data was initially disclosed, the data industry itself poses problems for the control over information once it is out of the hands of the individual. CIPPIC's 2006 study "On the Data Trail: How detailed information about you ends up in the hands of organizations with whom you have no relationship" revealed the complex personal information and data trade industry in Canada. Data collection agents obtain information on individuals through a range of tools and opportunities including product warranty cards, donor and subscriptions lists and the phone book. Once information leaves the control of individual and enters the labyrinth of the data industry supply chain, the individual has no control over where that data flows or its security.

Privacy and ethics concerns aside, the chart below illustrates the numerous points of secondary use, insecurity and exposure to vulnerability along the data industry supply chain from which individuals are incapable of protecting themselves. Individuals give their information to an assortment of legitimate organizations who become the primary data owners. Those data owners may also internally use customer data for marketing

¹²⁹ Roy Morgan Research, "Privacy and the Community" for the Australian Office of the Federal Privacy Commissioner (July 2001), online: <<http://www.privacy.gov.au/publications/rcommunity.html#1>>.

purposes or they may resell customer information to data compilers, analyzers or contact list managers. Depending on the business model, customer data may be infinitely resold to a wide variety of data agents. The users of this data are often direct marketing organizations, marketing research firms and charities. It is often impossible to ascertain the original or primary source of the customer personal information, who else has copies of the information or how many organizations have touched it before it ends up being used.

Diagram 3 - Data Supply Chain ¹³⁰

¹³⁰ Canadian Internet Policy and Public Interest Clinic (CIPPIC), "On the Data Trail: How detailed information about you ends up in the hands of organizations with whom you have no relationship" (May 2006), online: <<http://www.cippic.ca/documents/May1-06/DatabrokerReport.pdf>>.

These numerous, incredibly valuable databases are ripe plums for personal information thieves. Individuals have no direct control on the security and access protections over their information in the almost innumerable digital niches. Once the information is released, individual are relatively powerless to prevent its propagation or misuse. Once personal information is collected legally in the private sector, both the Canadian and US governments have legislation in place to covertly, but legally, obtain that information for state security purposes through the US *Patriot Act* and Canada's *Anti-Terrorism Act*.¹³¹ So while consumers may consent to information being used in the course of a commercial transaction, they are unaware that the information could also end up in the hands of national and international law enforcement.

While the chart illustrates difficulties monitoring the legal data supply chain that operates within the current legal framework, the illegal collection, interception and use of personal information is reaching epidemic proportions. According to the Strategic Counsel for the Competition Bureau of Canada, identity theft or marketing fraud has hit one out of every six adult Canadians, more than 4.2 million people.¹³² Two separate studies have indicated that internal employees commit 70% of information intrusions or security breaches.¹³³ Recent work done by Val Steeves as a part of the ORNEC IDT project illustrates the particular vulnerability of identity theft victims in a digital context.¹³⁴

¹³¹ *Anti-Terrorism Act*, S.C. 2002, c.41.

¹³² CBC News, "1 in 6 Canadians hit by identity theft, survey suggests" *CBC News* (1 March 2007), online: <<http://www.cbc.ca/consumer/story/2007/03/01/identify-fraud.html>>.

¹³³ Office of the Information and Privacy Commissioner of Ontario "Identity Theft Revisited: Security is Not Enough" (1 September 2005) at 24, online: <<http://www.ipc.on.ca/images/Resources/idtheft-revisit.pdf>>.

¹³⁴ Val Steeves, "Legal and Policy Approaches to Identity Theft" ORNEC Identity Theft Research Project Workshop II University of Ottawa (13 October 2006), online: <www.rilevis.com/seminars/feb07/Vsteeves_feb_2007.ppt>.

When individuals have their credit card stolen for example by a pickpocket, individuals are deprived of the single physical manifestation of their credit card. The victim is aware almost instantaneously of the loss and can take immediate action to contact the police and their bank.

However, in a digital context, the credit card can exist in multiple digital copies left distributed over a significant period of time and in locations not always known to the card holder (as illustrated in the diagram above). The victim cannot always reasonably know in which digital footprint the number was compromised. The number could have been copied months previously and resold. Often the victim does not have the benefit of knowing they have been 'robbed' until the fraud and resulting harm has actually occurred. At that point the harm is already been committed and the victim is not able to mitigate the loss or impact. Consumers who make online purchases or shop at stores who store customer data become more vulnerable as their digital footprints spread.

The foundation of modern privacy legislation and business practice are built on the assumptions that if you give people the tools to protect their privacy they will take the tools, want to, and be able to, use the tools. The research discussed above demonstrates these assumptions are flawed. Individuals have the least resources and understanding of the technology and business processes to protect themselves against the constant information request demands. Thus while both businesses and governments have built their personal information protection regimes on the notion of individual consent, it appears this is a weak foundation for effective governance.

The push back of responsibility primarily onto the individual also ignores the role and impact of societal, political and economic pressures. There are groups of individuals who are more vulnerable including children and youth, immigrants and people with limited education. Privacy pragmatists including Daniel Solove realize that privacy is one of many competing values and that people often trade privacy for other benefits including intimacy, efficiency and security.¹³⁵ We need to understand the real way people's privacy choices and behaviour are shaped and impacted by external forces such as technology, fear and ignorance as opposed to continuing to build a flawed theoretical foundation. An effective governance system would provide solutions and tools that would increase the ability of the individual to act more rationally while providing some protection for those individuals who are less able to protect themselves.

This section outlined three of the main assumptions associated with our current privacy protection regime. It illustrated that traditional conceptions of business motivation, individual capacity and legislative effectiveness are insufficient to protect personal privacy. What is needed is an informed, harmonized governance system designed to compensate for the identified weaknesses. This multi-party, multi-variable response will be discussed below.

¹³⁵ Solove, *supra* note 19 at 87.

Solving the Problem with Sustainable Governance

Once a problem has been adequately defined and understood, and misconceptions are clarified, it is then possible to conceive a process by which social issues can be rectified. Problem solving can be equally as daunting a task as problem identification.

Kernaghan Webb's model of sustainable governance provides a workable framework for more effective responses to privacy problems. According to Webb, the cornerstone of a sustainable governance approach is the meaningful alignment of the government sector, private sector and most importantly, civil society into governance roles. For clarification, in this thesis, individuals and Non-Governmental Organizations are considered to be part of civil society and distinct from actors in the government and business sectors.¹³⁶ This distinction is made, in part, to reflect the fact that, in contrast to many business actors- the motivation of many privacy civil society organizations is the pursuit of a collective social good that benefits everyone not just members.¹³⁷

¹³⁶ The London School of Economics Centre for Civil Society provides the following definition of 'civil society':

Civil society refers to the arena of uncoerced collective action around shared interests, purposes and values. In theory, its institutional forms are distinct from those of the state, family and market, though in practice, the boundaries between state, civil society, family and market are often complex, blurred and negotiated. Civil society commonly embraces a diversity of spaces, actors and institutional forms, varying in their degree of formality, autonomy and power. Civil societies are often populated by organisations such as registered charities, development non-governmental organisations, community groups, women's organisations, faith-based organisations, professional associations, trades unions, self-help groups, social movements, business associations, coalitions and advocacy group.

The London School of Economics Centre for Civil Society, "What is civil society?" (4 March 2004), online: <http://www.lse.ac.uk/collections/CCS/what_is_civil_society.htm>

¹³⁷ Colin Bennett, *The Privacy Advocates: Resisting the Spread of Surveillance* (Cambridge: MIT Press, 2008) at 27.

The private sector has come to understand that it is in their interest to be involved in the regulatory discussions surrounding their industries. As Webb illustrates, businesses are not interested in participating out of the goodness of their hearts; they are moved almost exclusively out of self-interest to grow market share, limit government regulations, and increase industry favourable outcomes. Government lobbying by industry is increasingly coming under scrutiny and has resulted in the establishment of a Lobbying Commission and the creation of a new federal *Lobbying Act* in the attempt to increase accountability and transparency.¹³⁸ As of March 2008 there were 1 754 corporate employees representing the interests of 283 different businesses and an additional 867 independent consultants registered as lobbyists with the Federal government.¹³⁹ While the exact monetary value of industry lobbying is not public knowledge, it is reasonable to conclude it is not only extensive, lobbying must have been determined to provide a worthwhile return on investment.

According to Webb, Non-Governmental Organizations (NGO) involvement in the policy process stems from a distrust in the abilities of the government and industry to effectively carry out governance activities. Individuals are motivated out of self-interest or a broader benevolent public interest. The history of the modern voluntary sector begins with recognition that there were gaps in government and business services.¹⁴⁰ Social welfare, health, education and environmental organizations have all emerged from grassroots origins to become established, funded institutions themselves. In 2008, non-profit

¹³⁸ *Lobbying Act*, R.S.C 1985, c. 44 (4th Supp.), as amended by S.C 2006, c. 9, s. 66.

¹³⁹ Office of the Commissioner of Lobbying of Canada, "Annual Report 2007-2008", online: <<http://www.ocl-cal.gc.ca/eic/site/lobbyist-lobbyiste1.nsf/eng/nx00319.html#s11>>.

¹⁴⁰ Children's Aid Society of Simcoe County, "History", online: <<http://www.simcoecas.com/en/aboutus/history.asp>>.

organizations registered 2439 lobbyists.¹⁴¹ However, the scope of the resources that a for-profit business can put into its activities far exceeds those of the non-profit sector or of individuals.

Webb's sustainable governance approach is premised on the concept that the government, business and civil society have a legitimate interest and capacity to take on governance functions. A governance system that is designed to incorporate the full range of government, corporate and civil society actors will be more effective. It will be better able to share the responsibilities, cost, learning and ability to respond to issues as they arise. Further, Webb asserts that governance responses that leverage the strengths of each actor will be more robust and therefore more effective and the solutions ultimately will be more *sustainable*.

Validating the participation of non-state actors does not take away from the important role of government. However, governments have inherent limitations. As noted above, legislative responses are usually slow, political and generally reactive. Legislative compliance often remains elusive. Even in an ideal scenario, perfectly constructed, timely, enforceable legislation remains insufficient on its own to address social issues. Sustainable governance posits a broader definition of governance instruments, institutions and processes beyond legislation. There are benefits of accommodating a wider set of actors, institutions, instruments and processes. In a sustainable governance approach, the

¹⁴¹ Office of the Commissioner of Lobbying of Canada, "Annual Report 2007-2008", online: <<http://www.ocl-cal.gc.ca/eic/site/lobbyist-lobbyiste1.nsf/eng/nx00319.html#s11>>.

role of government and legislation is enhanced and supported by the involvement of other actors.

Industry and individuals often have the capacity to respond quickly and to innovate solutions. Of course, as noted above, businesses also possess their own sets of limitations and weaknesses that impact their ability to engage in problem solving. Despite the limitations of all actors, the power and role of the government remains in a sustainable governance approach but is buttressed and infused with additional creative capacities and an expanded set of partners and tools.

Webb outlines how governance innovation can occur along three lines; institution, rule instrument and process. Each of these areas can overlap and work in cooperation with each other.¹⁴² An innovative institution is an organization that contains an observable public-interest component and assists in the facilitating the communication and transparency of the rules, enforcement or dispute resolution activities. Innovative institutions may provide access to or rely on citizen engagement activities such as petitions, complaints or publicity. An example of a governmental institution innovation is the Ontario Environment Commissioner that oversees the administration of an online information registry that posts links to decisions, draft decisions as well as facilitates citizen complaints leading to investigations.

¹⁴² The evaluation of the DNCL will articulate more fully how innovative institutions, instruments and processes can be engaged to address social issues.

Innovative rule instruments seek to influence or control behaviour and assess compliance through the techniques such as incentives, performance standards, voluntary codes or memorandums of understanding. An example of an innovative industry rule-instrument is the Canadian Scanner Price Accuracy Code which seeks to minimize errors in bar-code scanners. This program has been successful in part due to the incentives it contains for both consumers and businesses to be vigilant.¹⁴³

According to Webb, “processes are techniques that facilitate the ability of parties to participate in a meaningful and informed way in decision making that affects their interests.”¹⁴⁴ He distinguishes two forms of process innovations; those that facilitate access to information that assists parties to protect themselves and those that facilitate access to decision making including investigations, class-action and alternative dispute resolution. Industry Canada offers an early process innovation through its deployment of the Consumer Gateway, a central online service that links to over 400 government departments, agencies, industry associations and NGOs. As more consumers are moving online in their efforts to protect and inform themselves, this offering has proven very popular.¹⁴⁵

Webb also articulates that innovators under a sustainable governance framework need to understand the role and value of an appropriate level of rivalry, friction or creative tension. A sustainable governance approach does not require either consensus or direct conflict. Creative tension in a sustainable governance approach could inspire actors to

¹⁴³ Webb, *supra* note 48 at 258.

¹⁴⁴ *Ibid.* at 259.

¹⁴⁵ *Ibid.* at 260.

compete to develop better solutions. The need to manage rather than solve this creative tension in the context of privacy problems has been explored by Charles Raab through his privacy steering vision of the ‘race to the top’ introduced in “From Balancing to Steering: New Directions for Data Protection”.¹⁴⁶ Raab was one of the modern privacy academics who sought to articulate the process by which privacy can be managed on a practical level.

Raab specifically drew attention to a dominant conception that he termed the ‘doctrine of balancing’, a doctrine that fits directly into the liberal tradition. The ‘doctrine of balancing’ structures the privacy debate so that privacy protection in law is pitted against other, assumingly equal and competing values. Alan Westin can be viewed as strong contributor to the ‘balancing’ mentality. Westin wrote, “If privacy is to receive its proper weight on the scales in any process of balancing competing values, what is needed is a structured and rational weighing process, with definite criteria that public and private audiences can apply.....” The ‘privacy steering’ model suggested by Raab, moves away from a closed liberal approach. Instead of engendering a ‘one or the other’ approach, Raabs’ model allows policy or law-makers to approach the privacy issue in a more intuitive and responsive manner, leaning towards nuanced resolutions. Over a decade ago, Raab recognized that the future social and technological landscapes were unknown. Selecting one privacy approach or attempting to create a privacy balance ran the risk of stifling possibilities while a privacy steering model accepts and compensates for this uncertainty. Webbs’ sustainable governance extends this logic into a processed based,

¹⁴⁶ Charles Raab, “From Balancing to Steering: New Directions for Data Protection” in Colin Bennett and Rebecca Grant, eds., *Visions of privacy; policy choices for the digital age* (Toronto: University of Toronto Press. 1998) at 68-93.

problem-solving model. Civil society is not pitted against industry in their efforts to increase consumer protection, instead their dissent and activism helps strengthen overall privacy protection that will ultimately benefit business going forward.

One comparatively unexplored part of Webbs' analysis is the potential for individuals not part of civil society organizations to create new governance instruments, institutions and processes. When Webb discusses civil society, he seems to focus on NGOs or formal, coordinated actors. The rise of the individual activist empowered by the internet is a very recent phenomenon. As will be demonstrated in chapter four, Dr. Michael Geist, while a respected academic, is not a traditional NGO but has firmly inserted himself in the DNCL issue. Individuals, or *ad hoc* groups of individuals such as Facebook groups responding to the change in the Terms of Use have shown themselves to have power far beyond previous possibilities.¹⁴⁷ This adds an additional layer of complexity and opportunity for sustainable governance.

Privacy problems are a consistently moving target and the solutions designed to address them must be similarly adaptive. Webb understands that solutions evolve over time. Governance contexts can be understood first as immature with few characteristics of sustainable governance and then proto-sustainable, containing some of the characteristics associated with a mature sustainable governance approach. Proto-sustainable contexts may emerge haphazardly or accidentally without preconceived design or without

¹⁴⁷ "Facebook Bill of Rights and Responsibilities", online:
<<http://www.facebook.com/group.php?gid=69048030774>>.

systematic or coordinated framework. A fully mature sustainable approach conscientiously incorporates most of the innovative characteristics discussed above.

Innovative institutions, instruments and processes contribute to the development of an innovative governance regime. There are numerous examples of innovative institutions, instruments and processes in Canadian society working to address a range of social issues. Webb distinguishes sustainable governance innovations from traditional governance paradigms by considering a number of factors. These factors include whether the identified approaches work well with conventional approaches, recognize the importance of multiple centers of authority and responsibility, include elements of both policy development and implementation, harness an extended range of citizen, consumer, community, NGO and industry actors, and explicitly acknowledge the value of multi-actor collaborations.

A mature sustainable governance approach possesses most of the required characteristics and innovative institutions, instruments and processes. At present, there are no examples in Canada of mature sustainable governance approaches, but there are several promising examples of proto-sustainable governance containing examples of process, instrument and institution innovations. Webb discusses the current Canadian Consumer protection model as an example of a governance model on the path to sustainability. There are a number of traditional statutory and regulatory instruments in place including the *Competition Act*, the *Hazardous Products Act* and *PIPEDA*. Several industries including the banking and airline sectors have established Ombudsman offices to deal with

complaints and others, for example the Canadian Marketing Association and the Market Research Intelligence Association, have developed voluntary standards or codes of practice. Non-governmental consumer organizations have emerged including the Public Interest Advocacy Centre (PIAC) and SAC-Shawinigan, who developed an e-commerce certification program. These initiatives are starting points that can be built upon.

Embarking down a path towards sustainable governance, organizations are increasing working together to create multi-sector initiatives such as the Ombudsnetwork, a single-window access point to the complaints resolution services in the banking, health, life, securities and mutual fund industries. Webb notes that non-state actors and their voluntary activities exist partly in response to the threat or fear of government involvement. In other words, if an industry can be seen to be taking voluntary, pro-active measures they will be able to continue to operate on less formal regulation. Nonetheless, the voluntary basis of this industry association circumvented jurisdictional conflicts and therefore increased efficiency and assistance for the consumer.

In order to develop a robust sustainable governance model, Webb states that there needs to be an increased role of civil society actors. Citizens are increasingly engaging in social, political and public dialogues largely fueled by information and communication technologies.¹⁴⁸ However, government and private funding of the non-profit sector has decreased over the years and initiatives such as the Voluntary Sector Initiative were disbanded. CIPPIC, Canada's leading internet public interest foundations, has struggled every year for funds to continue its work as there is no current structure to provide stable

¹⁴⁸ *Ibid.* The Facebook bill of rights is an example of citizen engagement using social networking tools.

core funding. The analysis in Chapter Four will consider how PIACs' lack of resources inhibited their ability to become more involved in the DNCL process.

The federal governments' Sectoral Involvement in Departmental Policy Decision Making initiative provided direct funding to NGOs to contribute to the conversations around and creation of public policy. However, while this initiative was largely positive and increased NGO capacity, generally weak capacity of the NGOs to affect governmental department decision making as well as a lack of capacity for most departments to engage with NGOs and incorporate their expertise.¹⁴⁹

In an immature or proto-sustainable governance system, civil society actors are generally passive participants; they review proposals, make submissions or publicly complain after decisions are made. By contrast, in a mature sustainable governance system civil society civil society starts to develop and implement their own solutions and not just respond to the actions of others. In chapter four we will explore whether iOptOut represents an example of a mature Civil Society response to the DNCL.

Webbs' vision of a sustainable governance model provides several key elements that assist in solving privacy problems. First, no one actor can solve privacy problems on their own. Secondly, there are innovative ways of designing processes, institutions and instruments that are more effective than conventional approaches including governmental command and control. Third, each innovative institution, instrument or process is

¹⁴⁹ Human Resources and Skills Development Canada, "An Evaluation of the Sectoral Involvement in Departmental Policy Development (SIDPD)" (March 2004), online: <http://www.hrsdc.gc.ca/eng/cs/sp/sdc/evaluation/sp-ah214e/page03.shtml>.

strengthened by the involvement of other elements and creative tension can serve to increase overall performance. Finally, there is a central role for civil society to engage and produce their own robust solutions. These solutions may become fully aligned in the constellation of sustainable governance solutions.

Sustainable governance requires the development of a multivariable, multi-actor ‘ecosystem’ of solutions. Webb understands that his system requires that all interested parties come to the table to create a dynamic of “mutually assured implementation”. It is not articulated how to resolve open hostility or direct conflict between the parties. What happens when there are competing interests or principles at stake? While this omission does not invalidate the usefulness of the approach, further work will be needed to understand how best to apply it in a practical setting. Webb indicates that there may come a time when an industry voluntary code should be turned into a formal regulation. The DNCL is a perfect example and will be used in chapter four to illustrate the difficulties of navigating conflicting interests.

Next Steps

Thus far, traditional approaches and understandings of personal privacy protection have not been effective. There has been a systematic failure of business to develop robust privacy solutions. Partly due to a lack of *PIPEDA* compliance, we observe a failure of legislation to provide effective protection. The relative inability of individuals to protect themselves is evident. All these factors illustrate the shortcomings of the assumptions

behind the present system of privacy governance and point to the need for a multi-actor, multi-variable approach.

In chapter four we will explore the ways in which government's failure to adopt a sustainable governance approach may have contributed to its failure to adequately deal with the privacy problems that arise from telemarketing. In chapter five we will examine how adopting a sustainable governance approach may result in more effective solutions to these privacy problems.

Chapter Four: Case Study - Canadian National Do Not Call List

Chapter Summary

Telemarketing is generally understood to be the business or practice of marketing goods or services by telephone. The Canadian Radio-television and Telecommunications Commission (CRTC)¹⁵⁰ defines telemarketing as “the use of telecommunications facilities to make unsolicited telecommunications for the purpose of solicitation.”¹⁵¹ While cynics would state that the first telemarketing calls were made almost simultaneously with the first telephone call in 1876, the rise in modern telemarketing began in earnest in the 1950s and exploded in the late 1970s largely due to telecommunication advances pioneered by companies like Bell Canada. While traditional telemarketing involves a live-salesperson calling a potential customer directly, the practice has evolved to include predictive dialler technologies, automated voice messages and direct to mailbox messages.

¹⁵⁰ The Canadian Radio-television and Telecommunications Commission (CRTC) is the independent agency responsible for regulating Canada's broadcasting and telecommunications systems. As telemarketing falls under the domain of telecommunication, the CRTC has the regulatory oversight of telemarketing activities.

¹⁵¹ Canadian Radio-television and Telecommunications Commission (CRTC) “National DNCL Webinar Presentation” (24 September 24 2008), online: <<http://www.the-cma.org/PublicUploads/228620NationalDNCLCMASeptember24.pdf>>.

Today, telemarketing is big business in Canada. It is predicted that hundreds of thousands of businesses in Canada engage in some form of telemarketing every year.¹⁵² In 2000, the federal government recognized that ‘Customer Contact Centres’, which include telemarketing activities, are a lucrative contributor to the economy. The federal government created and funded Contact Centre Canada, the industry sector council.¹⁵³ The Canadian Marketing Associations’ own figures state that in 2006 alone, \$4.1 billion was spent on telemarketing, generating \$26.1 billion in sales and creating 155,000 direct jobs. As the telemarketing industry has increased, so too has consumer frustration and calls for solutions.

The process by which the Canadian National Do Not Call List (DNCL) came to be developed reveals much about both the conceptualization of the privacy problems related to commercial collection, use and disclosure of personal information and the privacy governance system in Canada. Telemarketing, a perceived nuisance by some and legitimate business by others, is an example of how a single issue contains a range and depth of theoretical, social and legal nuances. The DNCL process included the drafting of legislation, industry and public consultation over several years, as well as complex technical architecture, and business implementation against a backdrop of politicized manoeuvring. The Canadian DNCL provides fertile ground for examining how consumer privacy protection is conceptualized and actualized within a federally regulated industry.

¹⁵² CBC News, “Do-not-call list” *CBC News* (30 September 2008), online: <http://www.cbc.ca/news/background/telemarketing>.

¹⁵³ Contact Centre Canada, “Frequently Asked Questions”, online: <http://www.contactcentrecanada.ca/en/about-ccc/faq.aspx>.

The lessons learned from this case study can be transferred to other consumer privacy issues.

This chapter will outline the context in which the DNCL initiative emerged in Canada. The process by which the DNCL legislation was drafted and then implemented will be illustrated. Telemarketing and the DNCL solution will be examined in light of Daniel Solove's taxonomy of privacy problems. I will conclude by arguing that the DNCL initiative's failure to adequately address the issue of consumer privacy in telemarketing was caused by substantial content and process weaknesses. These failures motivated the creation of iOptOut.

Context of the Process and Development

In the attempt to provide proactive leadership around the issue of telemarketing and to stave off government regulation, the Canadian Marketing Association (CMA) assumed a leadership role in the telemarketing industry in the 1980s. The CMA developed a do not contact list, do not mail and do not fax list with an accompanying code of conduct.

Adherence to these guidelines was compulsory for all CMA members.¹⁵⁴

This attempt at voluntary industry self-regulation was largely symbolic. Membership in the CMA is not mandatory and only includes about 40% of marketing practitioners.¹⁵⁵

¹⁵⁴ The CMA has never attempted to establish a do not email list.

¹⁵⁵ Canadian Marketing Association, "Measuring the Return on Investment in the Canadian Marketing Association", online: <<http://www.the-cma.org/PublicUploads/223585MembershipInformation.pdf>>.

The CMA do not call list's status as a voluntary industry initiative left the CMA with few substantive penalties for violators and placed the organization in the difficult position of policing and sanctioning its own members. While most members complied with the CMA guidelines and used the established do not contact services, there was little interest or resources dedicated from the CMA to enforce the regulations. There remained a large percentage of the marketing industry who were not members of the CMA and were not interested in restricting their own activities or implementing consumer friendly telemarketing practices.¹⁵⁶ Throughout the 1980s and 1990s the telemarketing industry experienced exponential growth with corresponding levels of consumer frustration.

Despite the voluntary activities of the CMA to self-regulate telemarketing in Canada, consumer complaints about telemarketing continued to grow. Eventually the Canadian government came to recognize that stronger enforcement was required.¹⁵⁷ According to the CRTC, 20% or roughly 9000 of their complaint calls were regarding telemarketing.¹⁵⁸ The CMA encouraged the federal government to establish an official do not call list with investigation and enforcement powers. Around the beginning of 2000, the Canadian government began the process of developing a national do not call list at about the same time as other jurisdictions including the United States, United Kingdom, and Australia. The results reveal a slight diversity of models and process among the countries but for the most part the approaches adopted by different countries are comparable. There is a

¹⁵⁶ The Canadian Marketing Association, "Operation Integrity", online: <<http://www.the-cma.org/?WCE=C=47|K=224219>>.

¹⁵⁷ Canadian Radio-television and Telecommunications Commission (CRTC) "Telecom Decision CRTC 2004-35" (21 May 2004), online: <<http://www.crtc.gc.ca/eng/archive/2004/dt2004-35.htm>>.

¹⁵⁸ House of Commons Standing Committee on Industry, Natural Resources, Science and Technology, Evidence, 38th Parliament, 1st Session (20 April 2005), Richard French at 1540, online: <<http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=2583398&Language=E&Mode=1&Parl=39&Ses=1>>.

general acceptance that there should be a private-public partnership in the development, funding, administration and execution of any telemarketing complaints resolution process.

In 2003, the US National Do Not Call Registry was created and administered by the Government Solutions division of AT&T on behalf of the Federal Trade Commission (FTC), the nations' consumer protection agency. AT&T was awarded a 3 million dollar contract to establish the list as well as monthly billing for usage. The complaints procedure is managed and enforced by the FTC, the Federal Communications Commission (FCC), and state law enforcement officials.¹⁵⁹ The US National Do Not Call Registry while similar to that being deployed in Canada has a fundamental technology design difference that will be discussed below.

In the United Kingdom, the Telephone Preference Service (TPS) and the Do Not Mail service have been administered directly by the British Direct Marketing Association on behalf of the UK Office of Communications (OFCOM) since 2003. The complaints procedure is solely managed by the UK Information Commissioner's Office. This service is exclusively funded by the direct marketing industry. The British Direct Marketing Association also manages the do not mail service. Its corresponding organization the American Direct Marketing Association offers an email Preference Service (eMPS) but this service is not included in the UK legislation and it is a voluntary industry service.¹⁶⁰

¹⁵⁹ Federal Trade Commission, "Q&A: The National Do Not Call Registry" (July 2008), online: <<http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt107.shtm>>.

¹⁶⁰ Direct Marketing Association, "Contact Centres and Telemarketing", online: <<http://www.dma.org.uk/sectors/cct-introduction.asp>>.

In Australia, the comparable telemarketing legislation and service came into effect in 2006. The National Do Not Call Register and the initial complaints procedure is managed by a third party, Service Stream Solutions PTY Ltd on behalf of the Australian Communications and Media Authority (ACMA), similar to the CRTC in Canada. If a potential breach of the DNCR is found, the complaint will be forwarded to the AMCA for action.¹⁶¹ The operation regulations are similar to those deployed in Canada while the online technical registration is different.

The process by which the Canadian do not call legislation was envisioned, drafted, modified, enacted and ultimately interpreted and deployed reveals much about the status of privacy governance in Canada. Industry Canada, the department responsible for the development of the telemarketing legislation began investigations into the establishment of a do not call list at about the same time as many of the other international telemarketing legislative efforts and serious activity started around 2000. Over the next five year period, there was an extensive consultation processes and related activities. In May 2004, the CRTC issued Telecom Decision 2004-35 that sought to impose restrictions on telemarketing. The implementation of this decision was subsequently revoked after the CMA challenged the CRTC's authority to implement a national do not call list. Industry Canada responded in December 2004 with the introduction of *Bill C-37*

¹⁶¹ Australia Communications and Media Authority, "Do Not Call Register – Complaints and investigations" (December 2008), online: <http://www.acma.gov.au/webwr/_assets/main/lib310037/is154-dnccr-complaints_and_investigations-consumer.pdf>.

An Act to amend the Telecommunications Act which would give the CRTC the authority to initiate a national do not call list.¹⁶²

The legislation was given first reading in Parliament on December 13, 2004. The DNCL initiative was designed to be a public-private initiative with the government operating in a supervisory role.¹⁶³ Despite industry lobbying to the contrary, the legislation indicated that the funding and revenue of the DNCL would come solely from industry with no government funds allocated. The stated purpose of this delegation is to cut costs.¹⁶⁴

On April 13, 2005, the legislation was considered by the House Standing Committee on Industry, Natural Resources, Science and Technology (INDU). Initially Bill C-37, the DNCL legislation, contained no telemarketing exemptions. The original intent was that the legislation would provide the mandate for the creation of a do not call list and that the CRTC would then conduct a series of consultations on its operations, cost and exemptions, if any. In its first meeting, many INDU committee members including conservatives Werner Schmidt and Michael Chong indicated that they wanted exemptions to be included in the legislation, rather than dealt with through public consultations. The Industry Canada representatives believed it was more appropriate to let the CRTC establish the rules through public consultation. In her testimony, Denise

¹⁶² *An Act to Amend the Telecommunications Act*, R.S.C. 2005, c. 50. This will be referred to as the DNCL legislation.

¹⁶³ The ability to out-source the creation and operation of the Canadian DNCL stems from the Legislation amended in 2006. The changes to the *Telecommunications Act* (See section 41.1 to 41.7) included a section that allows the CRTC to delegate work out to a third party and allows the third party to charge for exercising its delegated powers *Telecommunications Act*, S.C. 1993, c. 38.

¹⁶⁴ House of Commons Standing Committee on Industry, Natural Resources, Science and Technology, Evidence, 38th Parliament, 1st Session (13 April 2005) Michael Binder at 1720, online: <<http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=1762702&Language=E&Mode=1&Parl=38&Ses=1>>.

Walter, Senior Counsel for the Department of Industry stated that it was their position that the regulations should be handled separately from legislation because:

...it's easier to change the rules as the need arises. CRTC officials have considerable experience and they can also hold public consultations before setting the rules. ... We want the public to have an opportunity to express its views on the matter before any rules are put in place.¹⁶⁵

On the second INDU committee meeting held April 20, 2005 the committee came prepared with amendments to include charitable and existing business relation exemptions.¹⁶⁶ The CRTC representatives demonstrated a reluctance to take a leadership role establishing the telemarketing regulations contrary to the earlier preferences of Industry Canada. Richard French, CRTC Vice-Chairperson stated:

With respect to exemptions, one major point that I would like to leave in the minds of the committee is that from the point of view of the commission, we would very much welcome the guidance of Parliament on this subject. It's extremely helpful to the commission to have Parliament pronounce on such questions of fundamental social values as what is and is not appropriate in the way of telemarketing.¹⁶⁷

In total, there were three public sector representatives who testified at the INDU committee representing Industry Canada, CRTC and the Office of the Privacy Commissioner. There were three organizations representing the charitable sector; Imagine Canada, Mothers Against Drunk Driving (MADD), and Canadian Council of the Blind. Three industry organizations testified; MRIA, Canadian Association of Optometrists and the Canadian Marketing Association. No consumer, academic or

¹⁶⁵ *Ibid.* Denise Walter at 1715.

¹⁶⁶ House of Commons Standing Committee on Industry, Natural Resources, Science and Technology, Evidence, 38th Parliament, 1st Session (20 April 2005).

¹⁶⁷ *Ibid.* Richard French at 1540.

privacy NGO organizations testified. After a total of seven meetings, on June 8, 2005 the Standing Committee on Industry, Natural Resources, Science and Technology proposed amendments to the original legislation that would include specific exemptions for charities, political parties, pre-existing business relationships, market surveys and newspapers.¹⁶⁸

The corresponding Senate committee considering Bill C-37 met even fewer times, with a total of two open meetings from November 15 to 23, 2005. The Senate committee called a total of seven witnesses of which only one was a consumer representative John Lawford from Public Interest Advocacy Centre (PIAC). The Senate report was one page long and only commented on the possibility of a reduction in fines.¹⁶⁹ The amended Bill C-37 received royal assent November 25, 2005.

Starting in February 2006, public consultations were held by the CRTC with formal presentations and submissions from mainly industry organizations with few consumer groups, notably PIAC, making submissions. The purpose of these consultations was to develop the operational requirements and regulations. These consultations did not recommend any substantive changes or modifications to the enacted legislation. The purpose of these sessions was to flesh out the DNCL regulations within the framework of the legislation.

¹⁶⁸ House of Commons Standing Committee on Industry, Natural Resources, Science and Technology, "Sixth Report" 38th Parliament, 1st Session (8 June 2005), online: <<http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=1916112&Language=E&Mode=1&Parl=38&Ses=1>>.

¹⁶⁹ Standing Senate Committee on Transport and Communications, "Ninth Report" 38th Parliament, 1st Session Government of Canada (22 November 2005), online: <<http://www.parl.gc.ca/38/1/parlbus/commbus/senate/com-e/tran-e/rep-e/rep09nov05-e.htm>>.

In March 2006, the CRTC formed two consortiums of interested parties – the Do-Not-Call List Operations Working Group (DOWG) and the Do-Not-Call List Implementation Working Group.¹⁷⁰ The vast majority of the participants on these working groups were industry representatives. On the DOWG there were seventeen industry representatives while there were only two consumer or citizen representatives – one of whom was an independent citizen representative. The reports from the DOWG were used to form the basis of the CRTC Request For Information (RFI) and Request For Proposals (RFP) that would be used to develop the DNCL technical infrastructure. The non-consensus report contained several items relevant to technology and privacy considerations. The issues debated in the group affected several fundamental technology and design decisions.

In July 2006, the CRTC took the Do-Not-Call List Operations Working Group reports and ran a Request For Information (RFI) from interested vendors and stakeholders. There were eleven responses that were to be used as a reference for the Request For Proposals (RFP). In December 2007, the contract was awarded to Bell Canada. The scope of the work included the development, implementation, and operation of the National DNCL as the CRTC's delegate. At present, the investigation, complaints procedure and administration are being handled by the CRTC. Despite intense lobbying, there was no governmental or CRTC funding provided for the development or operation of the DNCL. There was a nominal contract fee of \$1 and all DNCL costs were to be incurred by Bell Canada. In turn, Bell will receive subscription fees from the

¹⁷⁰ Do-Not-Call List Operations Working Group, "Report to the CRTC – Non-Consensus Report" (26 July 2006) at 48, online: <<http://www.crtc.gc.ca/public/cisc/do/DORE0001b.doc>> Referred to as DOWG Non-Consensus report.

telemarketing industry directly.¹⁷¹ The technical architecture was developed by Bell Canada and approved by the DNCL joint working group.

The DNCL rules appear relatively straightforward. Consumers must consent to be contacted by a telemarketer. If a consumer is on the DNCL, they should not receive any telemarketing calls, except from exempt organizations. Telemarketers are required to subscribe to the DNCL and ensure that they do not contact numbers on the list. The DNCL establishes penalties for violators in the range of \$1,500 for individuals and up to \$15,000 per violation for corporations per violation. The amounts can accumulate per day and per contact potentially resulting in very large fines. The money is currently directed into the general coffers of the government, not the CRTC, DNCL operator or enforcement agency.¹⁷²

In March 2008 Professor Michael Geist, Canada Research Chair of Internet and E-commerce Law at the University of Ottawa, decided to challenge the perceived inadequacies of the proposed do not call list head-on by creating and administering iOptOut. iOptOut is a non-profit website that will facilitate consumer opt-outs of both solicited phone calls and email marketing from both exempt and non-exempt organizations. The creation of iOptOut shocked and frustrated the leading industry players including the CMA, Canadian Bankers Association (CBA) and the Market Research Intelligence Association (MRIA). The CMA and CBA wrote formal letters of complaint to the CRTC while the MRIA commenced a defamation lawsuit against

¹⁷¹ *Ibid.* at 49.

¹⁷² National Do Not Call List, “Frequently Asked Questions”, online: <https://www.innate-dncl.gc.ca/faqs-eng#an_link09>

iOptOut and Michael Geist after he revealed that the MRIA had accessed the iOptOut list fraudulently.¹⁷³ To date, the CRTC has asserted that all organizations must comply with the iOptOut requests.

On September 30, 2008 the DNCL system became active. Both the phone and web-based registration systems were unable to cope with the volume of consumers attempting to register their phone numbers. It was reported that 1.5 million people attempted to register their number through the toll-free number but only 74,445 people were successful. Another 257,000 people registered online throughout the day despite the system repeatedly crashing.¹⁷⁴ Almost 4 million telephone numbers have been registered since the launch. There are 11.7 million residential phone lines and 16.7 million mobile phones for a total of 28.4 million phone numbers in Canada. Current DNCL registration represents 14% of total number of possible registrants.¹⁷⁵ iOptOut also saw a peak in registrations with over 1 million opt-out requests sent between September 30 and October 2, 2008.¹⁷⁶

On October 20, 2008, the CRTC announced that it was considering revising some of the telemarketing rules. Issues under examination include non-political party political calls, Automatic Dial Announcing Devices (ADADs) and harmonization with provincial

¹⁷³ Michael Geist, "Do-not-call faces challenges" *The Star* (9 October 2008), online: <<http://www.thestar.com/columnists/article/410819>>.

¹⁷⁴ Sarah Schmidt, "Glitches mark launch of 'do-not-call' registry" Canwest News Service (30 September 2008), online: <<http://www.financialpost.com/news-sectors/story.html?id=851194>>.

¹⁷⁵ Statistics Canada, "Quarterly Telecommunications Statistics 4th Quarter, 2005" Science, Innovation and Electronic Information Division Vol. 29, no.4 (May 2006), online: <<http://dsp-psd.pwgsc.gc.ca/Collection-R/Statcan/56-002-XIB/56-002-XIE2005004.pdf>>.

¹⁷⁶ iOptOut, "Do-Not-Call Registry Early Glitches" (2 October 2008), online: <http://ioptout.ca/index.php?option=com_multisite&Itemid=18>.

telemarketing legislation. It remains to be seen if industry lobbyists will be successful in inserting third party opt-out regulations or restrictions which would attempt to interfere with iOptOut's activities.

Within a few short months, problems with the DNCL began to come to light. In November, the CBC reported that thousands of Canadians were receiving more telemarketing calls after registering on the DNCL than they had received previously.¹⁷⁷ On January 14, 2009, Global TV revealed that the DNCL list was easily accessible to US telemarketers and fraudsters after an investigation revealed that a reporter could sign up and receive a copy of the list for \$50.¹⁷⁸ Conversely, a MRIA commissioned poll reported that Canadians were receiving fewer telemarketing calls.¹⁷⁹

The present DNCL initiative is but one of the possible privacy solutions to the telemarketing problem. Spearheaded by the CRTC in partnership with its industry developer and administrator Bell Canada, the DNCL grew out of a strong sector relationship particularly with the original Canadian Marketing Association in the context of a free market yet fiscally constrained political environment. Applying the lens of a privacy taxonomy and a sustainable privacy governance approach, we can observe how the actors, institutions, instruments and processes have come together to package a

¹⁷⁷ Canadian Broadcasting Corporation (CBC) News, "Thousands call to complain about do-not-call list" *CBC News* (27 November 2008), online: <<http://www.cbc.ca/consumer/story/2008/11/27/calling.html>>.

¹⁷⁸ Public Interest Advocacy Centre, "Do-not-call registry: Junk phone calls are down" (10 February 2009), online: <http://www.piac.ca/other/public_interest_news_government_safeguards_air_canada_fuel_fee_cibc_470_752_clients_best_toys_and_worst_of_toys_webkinz_and_neopets_bank_wal_mart_online_banking_bdus_sms_spam/>.

¹⁷⁹ Canadian Broadcasting Corporation (CBC) News, "80% of Canadians getting fewer telemarketing calls: survey" *CBC News* (9 March 2009), online: <<http://www.cbc.ca/consumer/story/2009/03/09/no-call-canada.html>>.

privacy solution to an identified privacy problem. It remains to be seen how, or if, the Canadian DNCL actualizes the consumer desire for privacy in their telecommunications.

Identifying Consumer Privacy Problems in Relation to Telemarketing using Solove

As noted above, the question remains whether the Canadian DNCL initiative will improve consumer privacy in Canada. To answer this question it is useful to return to the work of Daniel Solove. It will be argued that effective telemarketing protection first requires an appropriate understanding of the nature of the privacy problems associated with it. While consumer expressions of frustration at telemarketing could be seen to reflect a privacy claim grounded in the “right to be let alone”, a more nuanced understanding of the privacy problems allows for a more nuanced set of solutions.

As discussed in chapter two in his seminal book *Understanding Privacy*, Daniel Solove puts forward a new theory of privacy that is grounded in a specific context and focused on the ‘privacy problems’.¹⁸⁰ In the case of telemarketing, there are a number of potential privacy problems that arise. Understanding the nature of the specific privacy problem associated with telemarketing allows stakeholders to develop appropriate solutions.

According to Solove, it is necessary to recognize that privacy can be created. Solove notes that there is a distinction between the current status of privacy protections and our aspirations to privacy protections. Interestingly, Solove articulates that communication

¹⁸⁰ Solove, *supra* note 19 at 9.

privacy, like sleeping, bathing and toileting, is subject to socially constructed privacy conventions. “In other words, communications privacy was not a natural state the law preserved, but a form of protection the law created.”¹⁸¹ He chronicles how the social, technological and legal protections of ‘telegraph communications’ mirrors that of letters in the United States. In each, there was a desire for privacy of communications but there was concern that the technology (paper letters, phone line) was insecure and vulnerable to interception. Laws were passed by governments to increase protection and technology was created to decrease the risk.

For a long time, communications were vulnerable to interception, and their status could not always be ‘private’. The social desire, however, was for communications to be private even when they were not. In other words, we protect privacy with the tools of law and technology. Private communications could be protected through technology to meet the social desire for privacy. Therefore, to assess whether a particular practice or issue is private, we must look not only to the past and present, but also our future aspirations. Solove asserts that privacy is a condition we create; as such, it is dynamic and changing.¹⁸² A call for a process which allows consumers to remove their phone number and prevent unsolicited telemarketing is an example of a social desire to create personal privacy.

Soloves’ privacy taxonomy, or principles of classification, are used to describe a broad range of privacy problems. The first privacy problem that can be articulated in the

¹⁸¹ *Ibid.* at 61.

¹⁸² *Ibid.* at 64-65.

context of telemarketing using Daniel Solove's Taxonomy of Privacy is that of *Intrusion*. According to Solove, intrusion involves "invasions or incursions into one's life. It disturbs the victim's daily activities, alters her routines destroys her solitude and often makes her feel uncomfortable and uneasy."¹⁸³ Intrusion flows from the traditional 'right to be let alone' articulated by American legal scholars Warren and Brandeis. Intrusion can be equated with the sense of harassment when a person receives unwanted telemarketing calls.

In 2003, an Environics survey reported that 93% of respondents had a negative reaction to telemarketing. Telemarketing practices such as hang-ups, repeat calls, dead lines, or telemarketing phone calls during inconvenient times such as dinner, early mornings and bedtimes have contributed to citizens favouring intervention and regulation of telemarketing practices with 79% of the population wanting a national do not call list. On average, residents of Ontario received 4.54 telemarketing calls a week while Canadians with household incomes of \$80,000 or more received almost five calls a week.¹⁸⁴

People have evolved a range of behaviour changes to cope with telemarketing including screening calls for unknown numbers. Other strategies include waiting for the third ring to avoid the 'dead air' from predictive diallers.¹⁸⁵ Business has also responded by offering pay per use services for example call display and specific call privacy services -

¹⁸³ *Ibid.* at 162.

¹⁸⁴ Industry Canada, "Minister of Industry Tables Legislation for National Do Not Call List" (13 December 2004), online: < <http://www.ic.gc.ca/eic/site/ic1.nsf/eng/02336.html>>.

¹⁸⁵ Call for Action, "Do Predictive Dialers Violate Rules?", online: <<http://www.callforaction.org/tips/detail.asp?id=240>>.

at a cost of \$6.95 a month¹⁸⁶ as well as designing hardware to reject known telemarketing numbers.¹⁸⁷ It is obvious that consumers are impacted by the unwanted intrusion of telemarketing and they are actively looking for solutions to protect themselves and some businesses have responded by offering what could be considered a primitive PET.

The second privacy problem arising from telemarketing using Solove's taxonomy is *Insecurity*. In this context, Insecurity results from carelessness in protecting stored information from leaks and improper access.¹⁸⁸ As illustrated in chapter three, identity theft is one of the fastest growing crimes and once personal information is collected and in the hands of a second party, the individual loses effective practical control over that information. The documented misuse of the DNCL discussion validates consumer concerns about Insecurity.

Compounding the consumer frustration at telemarketing is a growing sense of consumer fear. Often unable to distinguish between 'legitimate' and illegal activities, Canadian consumers are falling for telemarketing fraud scams. From phoney charities, fraudulent contest winners to attempts at impersonating financial institutions, the telephone has become the next battleground of criminal activity.¹⁸⁹ PhoneBusters, a national anti-fraud collaboration, was initially established to target the growing phone-based fraud

¹⁸⁶ Bell Canada, "Call Privacy", online: <http://www.bell.ca/support/PrsCSrvPns_STSHelp_Details_CallPrv.page>.

¹⁸⁷ Privacy Corps, "Caller ID Information", online: <<http://www.privacycorps.com/pages/caller-id-information.htm>>.

¹⁸⁸ Solove, *supra* note 19 at 104.

¹⁸⁹ Phone Busters, "Recognize it", online: <<http://www.phonebusters.com/english/recognizeit.html>>.

phenomena. PhoneBusters has estimated that in 2008 to date, there have been 3928 Canadian victims of Mass Market fraud with a total monetary loss of \$16, 617, 532.33.¹⁹⁰

According to Solove, Insecurity exposes the consumer to potential future harm.¹⁹¹ The telemarketing industry has to be understood in the broader context of information collection, processing and dissemination: the data mining industry, the increasing digitization of activities and the value assigned to data by both legal and illegal actors. I would argue that Insecurity relates to both the technical vulnerability to harm as well as the psychological impact of that potential vulnerability. Consumers increasingly have a sense that they are vulnerable and therefore likely to be victims of identity theft.¹⁹² As such, people feel Insecure.

Telemarketing is largely possible because businesses actively collect the personal information of their customers as well as purchase potential customer lists. The collection of personal information by telemarketers triggers Solove's problem categories of *Surveillance*, the data collection gained by watching, listening or recording of information as well as *Interrogation*, the questioning or probing of information illustrate the passive and active forms of data collection. As illustrated in the- Data Supply Chain chart in chapter three, many consumers never know how their phone number gets into the databanks of organizations they have never done business with. The use of 'web cookies'

¹⁹⁰ Phone Busters, "Monthly Summary Report", online:
<http://www.phonebusters.com/english/documents/MonthlyStats_000.pdf>.

¹⁹¹ Solove, *supra* note 19 at 127.

¹⁹² UPI.COM, "1-in-10 Canadians hit by Web ID theft" (22 October 2008), online:
<http://www.upi.com/Top_News/2008/10/22/1-in-10-Canadians-hit-by-Web-ID-theft/UPI-37041224679643/>.

that allow web surfing activities to be tracked and reported back to the organization is a prime example of Surveillance. Many businesses use sophisticated Customer Relations Management software as well as mandatory data collection fields for web purchases. Examples of Interrogation include non-negotiable data fields and privacy policies that fail to give consumers the ability to opt-out of data collection when making a purchase or engaging a service. Dense and inaccessible privacy policies often hide the true extent of the data practices in a legal snowstorm of consent provisions leaving the consumer unaware or unclear of the surveillance or interrogation practices being conducted. There is no requirement that businesses establish the ‘providence’ of their consumer information or mandate explicit opt-in consent. In the business world today, extensive customer data is viewed as an asset.

The TJX-Winners debacle, one of the largest commercial data breach to date with 45.6 Million credit card numbers exposed, was compounded by to the over collection of personal information and then a systemic failure to safeguard that information.¹⁹³ TXJ-Winners, like most major retail stores today, try to install computerized Customer Relationship Management (CRM) systems that capture the customer personal data, shopping history, returns and overall analytics for use in business planning, advertising and marketing. Consumers are (supposed to be) asked to submit this data at purchase and few refuse. Some companies like Radio Shack make it difficult to make a purchase

¹⁹³ Murray Long, *PrivacyScan* (1 October 2007).

without giving personal information even while they are being brought up on charges relating to inappropriate data storage and disposal.¹⁹⁴

As chapter three illustrated, the business sector and the technology companies have failed to provide effective privacy solutions, safeguards or architectures. Almost weekly media releases of data breaches reinforce consumers' sense of Insecurity. Consistent and persistent Surveillance and Interrogation of consumers add additional fuel to the feelings of Intrusion. Telemarketing is an irritating and constant reminder of and contributor to Insecurity.

The last privacy problem that can be articulated in the context of telemarketing is larger issue of the right of consumers to control their personal information, in this case our phone number. Solove does not offer a taxonomy for any privacy problems arising from the individual themselves or violation of individual rights they could claim to. An argument could be made that *Secondary Use*, or the use of personal information for a different purpose than for which the data was collected without consent would apply. As illustrated in chapter three, the nature of individual 'informed' consent remains uncertain and problematic under current privacy governance regimes. CIPPICs' *PIPEDA* compliance study has effectively illustrated that privacy policies are inaccessible to the average consumer for the most part and that it is difficult if not impossible to 'opt-out' of affiliate or direct marketing data sharing consent requirements in privacy policies.

¹⁹⁴ Cynthia Marcotee Stamer, "Texas AG suit Against Radio Shack for Alleged Violation of 2005 Texas Identity Theft Law" *Risk Management and Compliance E-News* (10 April 2007), online: <<http://www.cynthiastamer.com/documents/alerts/20070409%20Identity%20Theft%20Updates.pdf>>.

Failure of the current DNCL response

In this section, I will demonstrate that the DNCL initiative fails to address many of the fundamental privacy problems associated with telemarketing, namely Intrusion, Insecurity, Surveillance, Interrogation or Secondary Use. It can be argued that the DNCL initiative was primarily perceived and designed as an initiative to regulate the telemarketing industry, not protect consumer privacy. Lacking a sound conception of the privacy problems at issue, the DNCL exercise therefore failed to address the substantive consumer privacy problems at the core of telemarketing. The legislation contained glaring omissions that failed to recognize the underlying consumer and social problems this legislation needed to address. The fundamental conceptual weaknesses in the legislation was coupled with a flawed technology implementation. The weaknesses in the results of the legislation and implementation were compounded by an insufficient process. It will be demonstrated that the process by which the legislation and regulatory approach came to be developed, revised and enacted failed to support or strengthen privacy protection thus created an inadequate solution. These problems were compounded by the wrong choice of technology to implement the system. A consumer anti-telemarketing initiative based on Solove's taxonomy of specific privacy problems that followed a sustainable governance approach would have potentially resulted in a set of more refined privacy legislation, technology choices and inclusive processes.

Content Problems

I will begin by considering the problems with substance of the DNCL solution. The initial legislation that was drafted by Industry Canada was heavily influenced by the historical precedents of the CMA do not call activities in Canada as well as the international legislative and operational precedents set by the US, UK and Australia. Rather than building on or advancing an innovative do not call service, the Canadian government chose instead to take a modest harmonized approach. As illustrated below, compared to the US technical deployment, the DNCL is an example of a less privacy progressive privacy solution. There was no legislative requirement to develop or even incorporate the highest privacy technical standards available.

As noted in the outset of this chapter, in 2005 the House of Commons Standing Committee on Industry, Natural Resources, Science and Technology (INDU) held public committee hearings to review the proposed legislation to amend the Telecommunications Act Bill-C37 which would allow the creation of the DNCL and establish the telemarketing rules. The initial proposed legislation drafted by Industry Canada differed greatly from the legislation that emerged at the end of the public consultation. In reality, it will be illustrated below that the INDU, Senate and CRTC public consultation processes resulted in less protection from Intrusion by allowing exemptions and did nothing to address other privacy issues such as Insecurity and Secondary Use by failing to address out-sourcing or consent requirements. The INDU committee did not hear from any consumer groups, largely ignored the recommendations of the Privacy Commissioner

including concerns about the charitable and existing business relationship exemptions,¹⁹⁵ and limited the appearances to pro-telemarketing organizations and charities championing DNCL exemptions.¹⁹⁶ The legislation was amended several times as a result of this process to contain several organizational exemptions.

One of the dominant criticisms of the DNCL legislation amendments that came out of the INDU committee was the addition of exempt organizations. Ultimately, this list included:

- Canadian registered charities;
- Political parties;
- Nomination contestants, leadership contestants or candidates of a political party;
- General circulation newspapers calling for the purpose of selling a subscription;
- To a consumer who has an existing business relationship with the organization;
- To a consumer who has given express consent to be called;
- Market research and polling firms;
- Business consumers.¹⁹⁷

As a result of these amendments, if an organization can demonstrate that they have an existing business relationship or consent to contact a consumer they are allowed to contact them. The legislation requires that explicit notice of consent to telemarketing and data sharing be given in the privacy statement. However, there is no requirement in the

¹⁹⁵ House of Commons Standing Committee on Industry, Natural Resources, Science and Technology, Evidence, 38th Parliament, 1st Session (8 June 2005) Jennifer Stoddart at 1535, online: <<http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=1915889&Language=E&Mode=1&Parl=38&Ses=1>>.

¹⁹⁶ Michael Geist, "Canada's Do-Not-Hesitate-To-Call List" (11 September 2005), online: <<http://www.michaelgeist.ca/index.php?option=content&task=view&id=950>>.

¹⁹⁷ *Telecommunications Act*, *supra* note 162, s. 41.7 (1).

legislation for plain language or severable out-in mechanisms to be used.¹⁹⁸ This means that all an organization has to do is add “telemarketing” to their already opaque privacy policies and they are free to continue business as usual relegating the whole DNCL exercise moot. Registered charities, newspaper circulation departments, market research and polling firms and political parties can continue to call consumers. The broad exceptions illustrate a failure to address the fundamental consumer privacy problems of Intrusion, Surveillance and Secondary Use. After the implementation of the DNCL, consumers are still going to experience intrusive phone calls, be subject to data collection and have their data shared without adequate consent. For many, the exempt organizations represent the very organizations that consumers do not want to be contacted by. It can be anticipated that consumers will be very frustrated if they continue to receive calls after registering for the DNCL due to exemptions.

The Canadian Marketing Association also successfully lobbied to have business-to-business telemarketing removed from the proposed legislation. The UK model restricts business-to-business telemarketing while the US model currently does not, despite individual State attempts to expand their List. The CMA fought against this inclusion because it would have set a precedent in North America and impacted severely the telemarketing industry. It was estimated that 60% of telemarketing is directed to businesses. According to Wally Hill, CMA Vice-President Communications & Public

¹⁹⁸ Canadian Radio-television and Telecommunications Commission (CRTC) “Telecom Decision CRTC 2008-6-1 Part V: Express Consent (20 October 2008), online: <<http://www.crtc.gc.ca/eng/archive/2008/dt2008-6-1.htm>>.

Affairs, “We argued that DNCL was primarily consumer issue and that in contrast the demand did not warrant it for businesses.”¹⁹⁹

In the attempt to protect and validate the telemarketing industry, the CMA worked hard to position the DNCL in the consumer domain and not include business-to-business telemarketing within its conception. Focusing on the general problem of Intrusion would have likely extended protection against business Intrusion and resulted in their inclusion in the legislation.

The issue of charities being included in the DNCL was hotly debated in the INDU. Consumer critics noted that it was the practice of telemarketing itself that was the problem, not the nature of the organization calling them. In other words, the problem was the Intrusion or ‘invasion of privacy’ itself, not the identity of the party that committed the Intrusion. Richard French, Vice-Chairperson, Telecommunications at the CRTC brought a report that was quoted as evidence in the INDU committee. He stated:

...the evidence brought before the Commission in its telemarketing public proceedings didn’t persuade it that there was any material distinction, in terms of nuisance, inconvenience and invasion of privacy, between a call made to solicit on behalf of a charity and one made to solicit on behalf of a commercial organization...²⁰⁰

¹⁹⁹ Brendan Read, “Canada: Third Party Do Not Call Exemption Collection OK” Contact Center Solutions (11 August 2008), online: <<http://callcenterinfo.tmcnet.com/analysis/articles/36571-canada-third-party-not-call-exemption-collection-ok.htm>>.

²⁰⁰ House of Commons Standing Committee on Industry, Natural Resources, Science and Technology, Evidence, 38th Parliament, 1st Session (20 April 2005) Richard French at 1550, online: <<http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=1789837&Language=E&Mode=1&Parl=38&Ses=1>>.

Professor Michael Geist took issue with the exclusions being added to the DNCL legislation dubbing the initiative the “Do-Not-Hesitate- to- Call List”. According to Geist, an estimated 85% of telemarketing calls would become exempt.²⁰¹ Charitable organizations lobbied in the INDU committee hearings not only to support their exemption under the DNCL but also to further broaden the federally registered charitable exemptions to include non-profit organizations.²⁰²

After it became clear that exemptions would be put into the legislation and not left to an independent CRTC consultation, Industry Canada representatives pleaded with the committee to establish some balancing mechanisms. During the INDU meetings, Industry Canada representatives proposed an amendment to split the DNCL and allow consumers to choose to opt out of receiving calls from charities separate from the main list. This recommendation would potentially have offered increased protection from Intrusion. However, the CMA lobbied against this option raising the fear that this requirement would lead to an increase in costs for both the DNCL and charities. John Gustavson, President and Chief Executive Officer of the Canadian Marketing Association testified in the committee hearing, “I’ve been advised within the last 24 hours by the people who administer our database that it could significantly increase the cost of DNC, and particularly increase the cost to charitable organizations.”²⁰³ This statement is specifically problematic as there was no architecture proposed or mandated within the legislation and

²⁰¹ Murray Long, *PrivacyScan* (29 September 2008).

²⁰² House of Commons Standing Committee on Industry, Natural Resources, Science and Technology, Evidence, 38th Parliament, 1st Session (4 May 2005) Peter Broder at 1645, online: <<http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=1823235&Language=E&Mode=1>>.

²⁰³ *Ibid.* John Gustavson at 1640.

there was no evidence that this decision would have had any, let alone significant, cost implications.

One of the second key consumer concerns that was overlooked by the legislation related to issues of Insecurity surrounding the out-sourcing of personal data to the United States. There has been consumer concern expressed about implications of the *US Patriot Act* on Canadian out-sourcing activities if the selected industry partner was a US company, or the industry partner subcontracts work to a US Company, or if the data resides out of Canada.²⁰⁴ At present, there is no requirement in the DNCL that Canadian personal data remains in Canada. This issue was discussed briefly in the House committee but ultimately a data residency clause was not added. The CRTC also considered these concerns in their consultations. However due to the various trade constraints including WTO and NAFTA, and in their perception the limited amount of personal information collected, the CRTC determined they could request that the data reside in Canada but they could not require it in the RFP. It was argued by the CRTC that a Canadian data residency requirement could be taken to the trade court as an undue disadvantage.²⁰⁵

Although the CRTC contractually requires that the DNCL contractor complies with both *The Privacy Act* and *PIPEDA* requirements, if the data were to be shared with any international data centre or service provider the ability to enforce the Canadian privacy legislation becomes near impossible. In the case of the US, the *Patriot Act* could be used to compel access to Canadian data being stored in the US as that legislation allows the

²⁰⁴ Canadian Broadcasting Corporation (CBC) News, "Patriot Act seen as threat to Canadians' privacy" *CBC News* (20 June 2006), online: <<http://www.cbc.ca/canada/story/2006/06/20/privacy-report.html>>.

²⁰⁵ Computing in Medicine Research Group Memorial University of Newfoundland, *supra* note 78 at 51.

government to gain access to any personal records held by an organization despite posted privacy policies.²⁰⁶

In the successful Bell Canada submission, the company voluntarily indicated that the data would remain in Canada and therefore remain under Canadian legal jurisdiction.

However, Bell Canada has indicated that a technical development partner is based out of the US. It is unclear at the point if the US sub-contractor accessed the data for development, testing or QA purposes. There is no requirement that data be de-identified for testing purposes or that the DNCL operator voluntarily anonymize data before it is released to any international technical partners in the legislation, operating rules set out by the DOWG or RFP. There is no certainty in upcoming contract renewals that the data will remain in Canada.

Treasury Board Secretariat (TBS), the governmental arm tasked with managing government operations, currently has no overt policy that requires Canadian government data to remain in Canada nor is there any other specific legislation or policy addressing Canadian data residency. TBS practices a 'risk mitigation' assessment and strategy. They are also in the process of developing voluntary guidelines.²⁰⁷ TBS does have a security requirement checklist that is used to determine the level of security protection required for technology initiatives. When consulted by the CRTC, the Public Works and Government Services Canada indicated that there was an informal threshold test asking

²⁰⁶ Treasury Board of Canada Secretariat, "Privacy Matters: The Federal Strategy to Address Concerns About the USA PATRIOT Act and Transborder Data Flows" (29 March 2006), online: <http://www.tbs-sct.gc.ca/pubs_pol/gospubs/tbm_128/pm-prp/pm-prp01-eng.asp>.

²⁰⁷ *Ibid.* at Section 6.

‘if the data was released to a US company what is the harm that could be done?’ The lack of clarity and strict interpretation of privacy risk is confusing for departments and decision makers and offered little assistance to under-resourced organizations like the CRTC.

There also appears to be little concern about the *Patriot Act* from the Canadian Privacy Commissioners. Ontario provincial Privacy Commissioner Ann Cavoukian was recently quoted as stating, “Fears associated with the Patriot Act are grossly exaggerated... This is a theoretical situation that might happen to your data residing in the U.S.”²⁰⁸ She called upon organizations to simply do due diligence on contractual agreements. Commissioner Cavoukian fails to validate the consumers’ feelings of fear, concern or anger. Many individuals have direct personal experience of state surveillance, oppression or retribution that has caused personal harm.²⁰⁹ These feelings deserve to be acknowledged and protected by decision makers. The lack of understanding of these privacy problems may lead to a failure to levy government resources to adequately protect privacy or provide a leadership role.

The exposure of Canadian consumer data to international governments illustrates several of Solove’s privacy problems including that of Intrusion, Surveillance and Secondary Use. Many Canadians would feel intruded upon if their data was accessed by a foreign

²⁰⁸ Brian Jackson, “Privacy controversy mars Google Apps rollout at Canadian university” *itbusiness.ca* (11 July 2008), online: <<http://www.itbusiness.ca/it/client/en/Home/News.asp?id=50660&PageMem=3>>.

²⁰⁹ The case of Maher Arar, the Syrian-Canadian who was deported by the US to Syria and was subject to torture is a prime example. Gus Hosein, “International Co-operation as a Promise and a Threat” in *Cybercrime and Jurisdiction: A Global Survey*, Bert-Japp Koops and Susan W. Brenner (The Hague: TMC Asser Press, 2006), online: <[http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-543297](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-543297)>.

government. In the aftermath of 9/11 and in the context of an enhanced global security movement, many citizens felt as though their government was not acting in their best interest. As the *Patriot Act* specifically disallows individuals to be notified that their data was accessed, this is an example of state Surveillance. Finally, while handing over data collected for the purpose of a commercial transaction to a government body may be legal, consumers may still feel it still indicates an inappropriate Secondary Use.

At the Senate level, the legislation was fast-tracked to receive assent prior to the Liberal Minority government falling. Senator Tkachuk, a former telemarketer himself, commented publicly that the House of Commons committee didn't conduct a full investigation into the matter and called upon his own committee to conduct a broader consultation.²¹⁰ There was little substantive discussion of the addition of the exclusions and none of the broader outstanding privacy problems were considered or debated. The senate's inaction and lack of leadership failed to compensate for the outstanding privacy problems in the amended legislation.

Once the legislation received royal assent, the DNCL initiative was handed over to the CRTC to implement. The next part of the process of establishing the DNCL was the creation of the Do-Not-Call List Operations Working Group (DOWG). This largely industry dominated group had the responsibility for making operation recommendations to the CRTC. It was these decisions that resulted in the version of the DNCL implementation ultimately deployed.

²¹⁰ Rob Hyndman, "Do-Not-Hesitate-to-Call is in the Senate" (5 November 2005), online: <<http://www.robhyndman.com/2005/11/05/do-not-hesitate-to-call-is-in-the-senate/>>.

The first technology decision was the technological alternatives and access architecture that the DNCL list would be built upon. There are two main methods. The first method ratified by the majority of the DOWG was the *download* method suggested and used by the CMA in Canada. This is the method used in the current Canadian DNCL. In this solution, the regulatory agency compiles a database of do not contact phone numbers that customers have registered. Telemarketers download that list of numbers to their own systems and then scrub their contact list against it. Telemarketers can then proceed to market to the remaining numbers. The stated advantage of this method is that it is simple, proven, cheap to implement, and many telemarketers already have the systems and processes in place to assimilate the requirements this type of DNCL because of their previous use of the CMA Do Not Contact service. The second design option championed by the minority but rejected by the majority of the DOWG, is a *query/response* method is a system in which a telemarketer would query the DNCL system with a number or a list of numbers they proposed to telemarket to. The DNCL system would then inspect the number(s) and inform the telemarketer if contact was permissible. The DNCL would not release or distribute the list of numbers outside the regulatory organization. This method is used in the United States and United Kingdom deployments. Proponents of this method assert this the more efficient, offers a greater revenue potential and is easier for small telemarketers to use. It also prevents the broad availability and circulation of the databases of registered phone numbers. Indeed, as predicted, the *download* designed DNCL was quickly demonstrated to be vulnerable to inappropriate use.

The second major design decision was the consideration of the difference between a “Do Not Call List” and a “Do Call List”. On a Do Not Call List consumers who do not want to be called are required to register their phone numbers. On a Do Call List consumers who want to be contacted would register their phone numbers. The DOWG minority argued unsuccessfully that the difference between a Do Not Call List and a Do Call List could be reconciled by conceptualizing the initial registration status of consumers: all consumers are on the list in a Do Not Call state until de-registered. It was asserted by the DOWG majority and confirmed by the CRTC that Bill C-32 only allowed for the creation of a Do Not Call list and that no other registry design was envisioned or permitted within the current legislation. The legislation, therefore, resulted in establishing de facto technology design decisions and imposed constraints on potential privacy innovations.

The DNCL legislation and technical implementation as they are currently deployed are not designed to address consumer privacy problems identified by Solove in relation to telemarketing. The legislation, particularly the exemptions, did not protect consumers against Intrusion. There were no substantive protections that would have mitigated against potential Insecurity and no requirement for clarity or conditions that would have prevented Secondary Use. The telemarketing industry, government and CRTC did not recognize the level of consumer frustration and anticipate their ability for independent reaction.

The iOptOut initiative discussed below is a direct civil society response to perceived legislative and implementation weaknesses. While it cannot address the technological and

out-sourcing vulnerabilities causing Insecurity and Secondary Use of the DNCL itself, iOptOut responds to the exemptions and issue of Intrusion not addressed in the legislation. Primarily iOptOut recognized that calls from exempt organizations constitute an Intrusion and sought to simplify and broaden a consumers ability to pro-actively withdraw consent to be contacted. Despite being behind its G8 counterparts in developing do not call legislation, the government and the key actors involved in developing the legislation did not foresee and therefore did not incorporate any provisions to respond to or incorporate third party actors like iOptOut intervening and taking independent action. The ways in which iOptOut may represent an innovative institution, instrument and process through its simplification of the ability of consumers to pro-actively withdraw consent will be discussed below.

Process Problems

The failure to address the privacy problems of Intrusion, Insecurity and Secondary Use was in part a result of process problems. As noted above, the DNCL initiative took years to complete. The creation of the legislation and regulations involved the department of Industry, the INDU, Senate committee and the CRTC public written and verbal consultation processes. The existing governance system deployed to manage the issue of telemarketing failed to first identify the privacy problems associated with the issue and then to appropriately engage actors, institutions, and instruments to solve it. Most importantly according to Webb's Sustainable Governance approach, the existing process failed to ensure meaningful participation of civil society. The lack of sophisticated

consumer engagement, coupled with the political and capacity vulnerabilities of the CRTC and government resulted in flawed telemarketing solutions.

It was evident that the Canadian CMA dominated the DNCL process from inception to deployment.²¹¹ The ability of the CMA to influence the development of the DNCL was largely due to a lack of capacity at the CRTC and a lack of political will at both the government and CRTC levels to restrict business or impact telemarketing revenues. While the CMA took a dominant role, its position before the CRTC and government was supported by other large and influential industry and charitable organizations. The relatively weak consumer voice was largely overwhelmed, out-maneuvered and out-resourced.

Similar to the CMA's heavy involvement with the creation of the legislation leading to Bill C-37, the CMA was heavily involved with the establishment of DNCL technology and operations framework. The CMA lobbied extensively to have the DNCL mirror existing business and technology practices. It was in the interest of the CMA to keep the technology design and process similar to that which its marketing members had previously operated under to avoid extra transition costs, industry confusion and prevent a more restrictive data sharing environment. Unfortunately, retaining the CMA operations model and easing the transition burden for industry prevented the possibility of the CRTC

²¹¹ Other than a handful of large corporations, few independent businesses in Canada have the interest and capacity to become politically involved in legislative initiatives. Most commonly, industry associations represent the interests of their sector organizations. Industry associations are usually self-funded entirely by industry, have the specific mandate to lobby levels of governments on behalf of the industry and employ lawyers, analysts and research departments to develop and communicate positions favourable to that industry. These industry associations carefully propose and monitor intended legislative initiatives. The Canadian Marketing Association is the largest coordinated industry association representing the interests of telemarketers in Canada

designing a next generation solution that could offer improved privacy protections. The wholesale adoption of the entrenched CMA DNCL technical model determined the fundamental direction for the privacy and technology decisions right from the outset.

From the beginning of its drafting, the legislation specifically allowed the CRTC to out-source the development and administration of the DNCL. The CRTC chose to exercise the option of out-sourcing for several reasons. First, the CRTC felt it did not have the internal capacity to develop and administer the list themselves. They had asked for and received the legislative power to delegate. Finally, as previously illustrated, there was an international precedent for out-sourcing DNCL operations in an era of increasing private-public partnership initiatives.

On the heels of a bloated National Gun Registry and the Secure Channel initiatives, it can be argued that government was leery of becoming involved in another funding 'boondoggle'.²¹² It is clear in the legislative amendments that it was government's intent that the telemarketing industry self fund the Canadian DNCL. This direct funding model was also used by the UK, Australia and to a different degree the US for their respective Do Not Call Lists. The CRTC receives its funding through fees imposed upon Broadcasters and Telecommunications Service Providers. The CRTC does not currently have the ability to collect funds from Telemarketers directly; neither did it seek to gain this ability through legislative amendment. Unlike the model in the US, Industry Canada

²¹² Kathryn May, "Government to replace \$1B online service 'boondoggle'" *Ottawa Citizen* (17 October 2008), online: <<http://www2.canada.com/ottawacitizen/news/story.html?id=53c07185-f270-4fca-b660-6b382bae2b16>>.

also chose not to provide start up funding for the DNCL initiative despite intense industry recommendation to that effect.

One of the implications of a lack of direct CRTC or government funding is that the CRTC felt it was unable to establish and insist upon specific architectures or technical requirements either within the legislation or after its enactment. The technical architecture of the DNCL is a fundamental component of the initiative. As there was no CRTC or government funding offered to initiate development, the cost recovery and revenue model created a situation where it is in the developer's best interest to develop and administer the system as cost efficiently as possible to maximize quick returns on investment. A cost minimization incentive could be said to contribute to a lack of corporate interest in implementing innovative privacy enhancing architectures and technologies.

There was a four year gap between when the CRTC formally commenced its investigations in 2001 and legislation was introduced in 2004. During this time, industry organizations were involved in extensive lobbying to provide exemptions for organizations and identified existing business relationships. The CMA was at the forefront of lobbying on behalf of telemarketers. In October 2006, the Market Research Intelligence Association (MRIA) conducted an intense 2 day Parliament Hill lobby and information day complete with a formal reception in the centre block.²¹³

²¹³ Market Research and Intelligence Association, "MRIA launches the world's first Charter of Respondent Rights" (3 October 2006), online: <<http://www.mria-arim.ca/STANDARDS/RespondentRights.asp>>.

The lack of internal capacity and over-reliance on industry partners in the government and CRTC is also established by the dependence on industry associations to provide wording for the legislation and accompanying regulations. When the MRIA was lobbying the INDU to have a research exemption added to the legislation, it hired a telecommunications lawyer to research and support its position as well as write a sample of legislative wording.²¹⁴ The government took and implemented the MRIA wording verbatim. The legislation not only excluded research activities from the DNCL, the legislation exclusively excludes research organizations from having to maintain and honour internal do not call lists unlike every other exempt organization.²¹⁵

In its March 27, 2006 submission the CMA states,

In this submission CMA suggests a set of telemarketing rules that we believe represent a fair, balanced and complete set of regulations for the telemarketing industry. Having said that, we recognize that other interested parties will have additional suggestions. The CMA respectfully requests the opportunity to comment on any other proposed telemarketing rules in addition to those detailed below before the CRTC issues its decision on the complete set of telemarketing rules.²¹⁶

The CMA was asserting itself as the primary expert on telemarketing without the benefit of external or neutral third party verification.

One instrument used by government intended to assess privacy impacts is a Privacy Impact Assessment (PIA). Generally, a Privacy Impact Assessment (PIA) is a formal

²¹⁴ Market Research and Intelligence Association, "Telemarketing Do-Not-Call Registry Becomes Law . Major Win For Survey Research" (25 November 2005), online: < <http://www.mria-arim.ca/NEWS/Telemarketing.asp>>.

²¹⁵ *An Act to Amend the Telecommunications Act*, S.C. 2005, c. 50, s. 41.7 (1)(f).

²¹⁶ Canadian Marketing Association, "Letter to CRTC Re: Telecom Public Notice CRTC 2006-4" (27 March 2006), online: <http://www.crtc.gc.ca/public/partvii/2006/8665/c12_200601626/606961.pdf>.

investigation designed to identify the privacy issues involved in an initiatives and ensure that privacy principles are considered in planning organizational activities.²¹⁷ The role of a conceptual or technical PIA is to identify privacy policy and technical requirements in advance. There is no systematic process by which legislative amendments are vetted against privacy other than the public process by which the legislation is created and discussed in the department, committee and ultimately the house of Parliament. There is no formal requirement that government conduct a formal PIA on any legislative activities. If there are flaws or oversights in the legislation, subsequent activities including PIAs are hampered or unable to address them. A PIA as a tool can only work within the legislative framework as it exists.

The TBS guidelines require a PIA be conducted for all government initiatives as a requirement for funding but there is no specific criteria for the PIA, timeline, or implementation. Neither PIA activities nor privacy legislation are formally and consistently structured to address privacy problems as articulated by Solove. The absence of an approach grounded in privacy problems weakens the PIA instrument and process. A conceptual PIA should include the major policy and business issues that must be considered as the project progresses as well as identify the privacy problems arising from the activities. All subsequent project actions should alleviate the identified problems. A technical PIA should identify the specific technical and policy implementation privacy problems arising based on an established technology taxonomy such as Soloves'. In the

²¹⁷ Treasury Board of Canada Secretariat, "Privacy Impact Assessment Policy" (2 May 2002), online: <<http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12450§ion=text#cha3>>.

construction of the DNCL legislation, there was no requirement for a limited conceptual or technical PIA to be conducted.

In 2006, the consulting group of the Public Works and Government Services Canada (PWGSC) recommended to the CRTC that a conceptual PIA be done.²¹⁸ The CRTC felt it did not have the resources to conduct a conceptual or technical PIA internally and chose not to make a strategic or proactive investment in them. Misunderstanding the role or opportunity of a conceptual or technical PIA, the CRTC did not feel that a technical PIA was necessary because the technical architecture was to be developed by the industry partner. The industry partner was not selected until well down the process resulting in substantial process, policy and design decisions being made de facto in the absence of any privacy design criteria.

In fact, up until 2 months prior to the launch, the PIAs had not been completed. The chosen industry partner Bell Canada was responsible for conducting a systems and operational PIA pursuant to Treasury Board Secretariat guidelines. The CRTC was responsible for conducting a PIA for the investigations and complaints process. Due to a lack of internal capacity, the CRTC hired Bell Canada to do their PIA on its behalf.²¹⁹ Both PIAs were to be submitted to the Office of the Privacy Commissioner for review but this will accomplish little as the system will already have been developed and deployed. The lack of a specific requirement in legislation for a conceptual PIA based on articulated

²¹⁸ Computing in Medicine Research Group Memorial University of Newfoundland, *supra* note 79 at 55.

²¹⁹ *Ibid.*

privacy problems leads to missed opportunities to make strategic decisions at a point where cost effective and efficient privacy solutions can be implemented.

Failures of the process contributed to flawed technology decisions. These decisions were not designed to protect consumer or privacy interests. For example, there was a specific discussion in the DOWG about limiting telemarketers' access to the DNCL.

The Majority was of the opinion that there was no security or privacy risks in the DNCL Operator implementing technology that would permit a telemarketer to download all or a portion of the DNCL....The Minority remained concerned that telemarketers should not be able to download the DNCL from the Operator because of the privacy risk of telemarketers having confidential telephone numbers.²²⁰

As industry dominated the DOWG, they were able to act in their own self-interest. The industry dominated DOWG majority asserted that there was no logic in the prevention of the release of customer phone numbers. They asserted that telemarketers simply wouldn't bother to contact people who had expressed a preference for not receiving telemarketing calls. In light of the strengths and weaknesses of both methods discussed in the group, the majority felt that bidders for the DNCL Operator contract should investigate both download and query/response design proposals and determine the feasibility of either method, or a combination of both. The minority noted that permitting a commercial process to determine technology is in effect allowing them to determine public policy. The minority also believed that this type of fundamental design decision, which concerns the nature of a work solely intended to protect the public, should not be undertaken by the

²²⁰ Do-Not-Call List Operations Working Group, *supra* note 179 at 4.

CRTC without carefully considering the opinion of well-qualified, impartial, registered professional engineers.

As discussed in chapter three, behavioural science and common sense dictates that human behaviour is such that there will always be a segment of the population who will not or cannot act on their own behalf and therefore a Do Not Call list will not proactively protect those consumers. Conversely, a Do Call List will contain significantly fewer people and drastically negatively impact the telemarketing industry. Again, the balance of protection tilted in the direction of the telemarketing industry, not consumers. We will observe in the next section how the legislative framing directed the policy and technology opportunities and outcomes from the outset.

If decision makers decide that phone numbers are in and of themselves innocuous then the privacy considerations they place on them will be correspondingly small. This decision reinforces the perception that decision makers do not conceptualize telemarketing as overly Intrusive or understand the Insecurity associated with the leaking of phone numbers as particularly problematic. However, if decision makers contextualize those phone numbers themselves within the broader constellation of other data banks, reverse look up technology and re-identification attacks individual data points could become viewed as increasingly sensitive and worthy of protection.

It is interesting to note that in the balance of problems and harms between consumers and industry, the DOWG was more concerned with impact of misuse on industry. There were recommendations in the consensus report to implement technical solutions against

‘mistakes and mischief’ specifically to prevent mass fraudulent registration on the DNCL. Phone registrations were required to be made from the numbers being registered and online registrations were limited to 3 fields and an automatic code generator registration ticket be added to minimize automated registrations.²²¹ There were no specific recommendations made for requiring technologies for protecting the DNCL database. There are numerous privacy and security solutions that could have been required including digital ‘watermarking’ of DNCL databases as to determine the provenance of the lists if leaked, mandating specific encryption provisions, or implementing access auditing procedures. There is no requirement for telemarketers to track or inform the CRTC if they know or suspect that their list has been breached. While not exorbitant, these requirements would have taken additional resources for telemarketers to implement, monitor or enforce. These oversights lead to at best a failure to mitigate and at worst a potential increase in Insecurity and Secondary Use.

The role and value of involvement of privacy technology experts was not noted by the committee in either report and there was no recommendation that privacy technology experts review potential technology designs. There was no recommendation that a list of potential privacy and security solutions with their potential costs be developed before a Request For Information (RFI) or Request For Proposals (RFP) was issued. It was left to industry respondents to put forward privacy solutions. A parallel CRTC Consortium was supposed to develop a Request for Information (RFI) questionnaire that would ask potential respondents to describe their capabilities and any preliminary views that they

²²¹ Do-Not-Call List Operations Working Group, “Report to the CRTC – Consensus Report” (26 July 2006), at 3, online: <<http://www.crtc.gc.ca/public/cisc/do/DORE0001a.doc>>.

may have concerning the operation of the proposed DNCL system. It was anticipated that the Consortium would assist the development of the RFP before other technical, operational and administrative decisions were made.²²² However, the overwhelmingly industry based Consortium folded after they felt that they would be in a conflict of interest as many of the players were interested in bidding on the contract or they felt participating in the Consortium would make them potentially liable for operational costs.²²³ The RFI proceeded to be issued without specific guidance around consumer privacy.

In July 2006 the CRTC took the Do-Not-Call List Operations Working Group reports and ran a Request For Information (RFI) from interested vendors and stakeholders. There were eleven responses that were used as a reference for the Request For Proposals (RFP). While some responses went into great technical details as to what code and tools would be utilized, others were more general in their comments. While the RFI asked for general comment on privacy protection options, none of the industry respondents commented directly on how they would address privacy. All vendors proposed a version of the download model. Additionally, none of the respondents proposed any of the alternative privacy enhancing query/response or 'List scrubbing' DNCL models or architectures. There were no technical solutions presented that would have addressed consumers concerns of potential Secondary Use or Insecurity. The lack of privacy preserving architectures and technologies at this stage further limited the articulation of the final

²²² Canadian Radio-television and Telecommunications Commission (CRTC) "Telecom Public Notice 2006-4" (20 February 2006) # 29, online: <<http://crtc.gc.ca/eng/archive/2006/pt2006-4.pdf>>.

²²³ Do-Not-Call List Operations Working Group, *supra* note 222.

technology requirements in the RFP.²²⁴ The CRTC relied extensively on the expertise of external personnel to articulate the privacy requirements and obligations in the RFP. They engaged outside legal counsel and RFP consultants who specialized in government contracts to help develop the RFP and identify requirements. The Office of the Privacy Commissioner was asked to give informal, off the record guidance. Again relying on external expertise, the PWGSC wrote the RFP on behalf of the CRTC.²²⁵

Specific privacy technology requirements were not fully articulated for the venders in the RFP. Dense and vague Treasury Board Secretariat documents and the antiquated *Privacy Act* were referred to and it was left to the respondents to translate the requirements into actions and design decisions. Incorporating the above information as well as the DOWG reports, the bulk of the provided preliminary technical requirements outlined were supplied by the CRTC.²²⁶ The CRTC in its decision 2007-48 specifically noted that they did not believe it was appropriate for them to restrict the Operator to specific technology or methods.²²⁷ It was clarified by the CRTC that vendor must understand their privacy responsibilities on their own using their own access to professionals. The CRTC will ensure that the vendor complied with the privacy obligations through the PIA to be performed, performance audits, as well as third party security audits. There was an oversight committee formed with representatives from both Bell Canada as well as the CRTC who reviewed and signed off design documents and progress reports. As the

²²⁴ Computing in Medicine Research Group Memorial University of Newfoundland, *supra* note 78 at 54.

²²⁵ *Ibid* at 54.

²²⁶ *Ibid* at 54.

²²⁷ Canadian Radio-television and Telecommunications Commission (CRTC) "Telecom Decision 2006-4" (20 February 2006) at 1142, online: <<http://crtc.gc.ca/eng/archive/2006/pt2006-4.pdf>>.

contract is only for a nominal \$1, if a breach of contract occurs there may be limited recourse.²²⁸

As with the RFI, there were no innovative privacy solutions presented from any of the respondents in the RFP. Because there were no mandatory privacy technology requirements, the motivation for innovation was left with the vender at the same time as there no direct financial compensation associated with it. The CRTC didn't feel it had the knowledge or capacity to mandate specific technology solutions. The CRTC evaluated the proposals based on relevant experience.²²⁹

In preparation, Bell Canada assembled a legislative review team to follow the development of the DNCL Legislation as well as an internal proposal development team. While Bell privacy experts were involved with the initiative, it was evident from the results that their effectiveness was hampered by the CMA architecture legacy, lack of internal willingness to redesign the DNCL architecture, limited budget and an overwhelming corporate profit maximization motive.

The third and most substantial failure of the process is the lack of full participation by civil society, consumer or non-government, non-industry stakeholders. As a part of the DNCL process the House INDU committee, Senate committee and CRTC conducted hearings and requested written submissions from interested parties. The overwhelming majority of respondents were from industry. As outlined above, the Do not call list

²²⁸ Computing in Medicine Research Group Memorial University of Newfoundland, *supra* note 78 at 55.

²²⁹ *Ibid.* at 55.

Operations Work Group (DOWG) members were also predominantly from industry (seventeen) with only one consumer representative and one individual representative. It has been argued that the lack of substantive civil society or consumer involvement weakened the legislation and technology solutions presented.

Consumer and civil society organizations are relatively weak in Canada. There are few consumer or civil rights organizations in Canada and there are even fewer dedicated Privacy organizations. Most NGOs operate with limited budgets and few resources. The Public Interest Advocacy Centre (PIAC) was previously noted to be heavily involved in the CRTC regulation space in the past largely due to the fact that organizations are financially reimbursed for their participation and involvement. However, PIAC did not take on as active a role as they could have exercised in the DNCL process. Like most NGOs in Canada, PIAC suffers from limited personal and resources. It could be concluded that upon review of the initial process and offering, PIAC observed that the proposed DNCL system had already been heavily dominated by the telemarketing industry association and contained too many sector exemptions to be effective. Even though there was some possibility of financial compensation, PIAC may have felt that the proposed DNCL system was unwaveringly committed to following industry lead that there was no possibility of steering the initiative back to a consumer friendly path. Similarly, the Consumers' Association of Canada has done little to no work on telemarketing complaints. Their website has no information available.²³⁰

²³⁰ Consumers' Association of Canada, "Telecommunications", online: <<http://www.consumer.ca/1530>>.

The public consultation processes for the DNCL legislation conducted by the House INDU committee, the Senate committee and CRTC was largely symbolic. While there was a process in place to include the public, the vast majority of respondents held a direct financial stake in the continuation of telemarketing with the least possible restrictions. There was no requirement or incentive for any of the institutions to conduct a balanced consultation.

The lack of substantive involvement by consumer or civil society resulted in a weakened legislation, poor technology and operational decision and ultimately failed to address any of the privacy problems articulated by Solove. Consumer frustration with intrusive telemarketing was set aside in favour of not impacting the telemarketing industry or limiting charitable fundraising. Consumer concerns about insecurity were ignored in favour of preferring of industry convenience and profit. Consumer vulnerability to state and industry secondary use was also overlooked. The lack of civil society involvement in the process continued until the emergence of iOptOut.

I Opt Out

Frustrated with the DNCL process, Professor Michael Geist, Canada Research Chair of Internet and E-commerce Law, launched his own do not call solution – iOptOut in March 2008. Using funds allocated from his research chair position, iOptOut was designed and launched as an applied research project. iOptOut is a web-based application that allows consumers to create and manage a personal do-not-call list specifically for organizations

exempt under the law. Offering a more nuanced technological approach, consumers can register and opt-out of exempt organizations, withdraw consent from organizations from which consumers can be said to have a pre-existing business relationships as well as proactively deny consent from organizations. Consumers indicate their contact preferences and iOptOpt emails the selected organizations on the consumers' behalf.

iOptOut offers increased protection from the privacy problems of Intrusion and Secondary Use. Consumers become empowered to remove themselves from contact lists of organizations from which they do not wish to receive telemarketing. Because of complicated privacy and terms of use contracts, consumers can also opt-out of telemarketing from organizations they may not have realized their information had been shared with and therefore reduce unintended Secondary Use. Finally, consumers can proactively limit calls from organizations they never wish to have contact with. Most interesting, iOptOut allows consumers to allow contact with sectors and specific individual organizations. This initiative has the added bonus of increased public participation through their blog and wiki. Consumers can control and observe the organizations they selected. Consumers can also nominate new organizations to be added to the list.

iOptOut has the added bonus of allowing consumer email addresses to be added to organizational internal do not call lists. Currently the DNCL does not address email solicitations and Canada is the only G7 country with no national unsolicited email

(SPAM) legislation.²³¹ iOptOut draws its authority from *PIPEDA*. Under *PIPEDA*, businesses must respect the withdrawal of consumer consent. There are provisions for consent to be managed by an agent on behalf of the consumer.²³²

Some industry groups have reacted with considerable outrage toward iOptOut.ca. For example, both the Canadian Marketing Association (CMA) and the Marketing Research and Intelligence Association (MRIA) initially advised their members that they may be able to ignore Canadians' opt-out requests since the requests were not 'authenticated'. They offered members response scripts in response to iOptOut inquiries and sample privacy policy clauses disallowing third party opt-outs.²³³ The Canadian Bankers Association (CBA) supported the CMA in a written submission to the CRTC and in letters submitted to national newspapers.²³⁴ Both the CMA and CBA have gone on the record that telemarketing is an important part of their business activities. In its submission to the CRTC in response to CRTC decision 2004-35 the CBA specifically asks the CRTC to exempt banks and their financial institution affiliates from the do not call legislation, a comment not indicated in their public letters.²³⁵

²³¹ Michael Geist, "Lawless Canada Emerging as a Spam Haven" (1 December 2008), online: <<http://www.michaelgeist.ca/content/view/3552/159/>>.

²³² iOptOut, "Enforcing Your Opt Out", online: <https://ioptout.ca/index.php?option=com_content&task=view&id=9&Itemid=20>.

²³³ Market Research and Intelligence Association, "MRIA Member Advisory On iOptOut.ca" (2 August 2007), online: <<http://www.mria-arim.ca/INDMEMBERONLY/CorpAdvisory-08-02-07NP.asp>>.

²³⁴ Nancy Hughes Anthony, "Banks are in favour of national Do Not Call list" *The Vancouver Sun* (8 August 2008), online: <<http://www2.canada.com/vancouversun/news/letters/story.html?id=0b7dbacf-ef55-4b58-b5f2-619904a891d4>>.

²³⁵ Canadian Bankers Association, "Submission of the Canadian Bankers Association CRTC File: 8662-C131-200408543" (07 September 2004), online: <<http://www.crtc.gc.ca/public/partvii/2004/8662/cba/040907.zip>>.

Faced with fierce criticisms that iOptOut would become a haven for ‘radical privacy and cyber activists’, questions were posed by the CMA and CBA to the CRTC concerning the process by which phone numbers are registered on iOptOut. iOptOut asserted that it had both the force of the DNCL and *PIPEDA* legislations in its favour. Under the current DNCL regulations, there is no requirement for a procedure to authenticate the person registering with the DNCL. In an attempt to cut technology costs and ease registration at the time, the CRTC previously deemed that the likelihood that someone would falsely enter someone else's phone number in an on line registration was minimal. This aspect of the DNCL follows the examples of other international opt-out lists including the U.S. FTC's Do-Not-Call list and the CMA's own do-not-market list who do not authenticate the link between the user and the registered phone numbers.²³⁶

The CMA and CBA also levied criticisms that the email to iOptOut from consumers and from iOptOut to third party organizations is not secure and exposes the customer to email fraud. This is a legitimate claim. But the vast majority of all email transmitted is insecure and vulnerable to illegal and accidental sniffing.²³⁷ It is illuminating that the CBA is using claims of the immaturity of the technology to prevent consumer protection, when, as demonstrated in chapter 3, industry has done little to no work to raise the bar of email privacy or security generally. Geist and his team responded by increasing security and meeting with representatives in an attempt to develop mutually satisfactory solutions for businesses to handle incoming iOptOut requests.

²³⁶ Michael Geist, “CMA and MRIA Recommend Against Respecting iOptOut Requests” (8 April), online: <<http://www.michaelgeist.ca/content/view/2820/135/>>.

²³⁷ PCtools, “Email insecurity highlighted by Lord West” (26 March 2009), online: <http://www.pctools.com/industry-news/article/email_insecurity_highlighted_by_lord_west-19092984/>.

It was evident that the CRTC and telemarketing lobbying community did not anticipate a parallel consumer driven do not call instrument. No one from government or industry foresaw a tool with the ability to rapidly process large volumes of requests on behalf of consumers. The legislation, technology requirements and operation rules were written for the scenario of a single administrator interacting with registered telemarketers to service dispersed and fragmented individuals. The legislation is completely silent on the possibility and role of independent third parties. iOutOut operates on the premise that the DNCL legislation does not restrict third party consumer opt-out registration and that all requests must be honoured with the same respect as direct requests under *PIPEDA*.

There is previous recognition about the limitations of the powers of individuals through the emergence of the use of agents or proxies. In some situations including health and safety, government pre-emptively intercedes on behalf of individuals. Proxies allow third parties to take on governance responsibilities on behalf of others.

After the launch of the DNCL and iOptOut in the face of the industry response, CRTC chair Konrad von Finkenstein concluded that iOptOut is not precluded from operating and that industry organizations must honour iOptOut requests.²³⁸

In its endorsement of iOptOut von Finkenstein formally responded to the CMA and CBA noting that neither the Unsolicited Telecommunications Rules nor the DNCL legislation

²³⁸ Canadian Radio-television and Telecommunications Commission (CRTC) Letter to the Canadian Marketing Association “Re: Do Not Call requests made through iOptOut.ca Reference # 392251” (27 June 2008), online: <http://www.michaelgeist.ca/component/option,com_docman/task,doc_download/gid,19/>.

precluded a consumer from pro-actively opting out of receiving telecommunications. Further, he noted that CRTC Decision 2007-48 did not set any restrictions on the method by which opt-out requests were made. Despite industry claims that the iOptOut requests were vulnerable to fraud, the CTRC clarified that iOptOut is subject to the same verification requirements as the DNCL - namely that there are no verification requirements in either the legislation or technical design. In the effort to keep costs down, simplify registration execution consumers and telemarketers and in the face of limited required technical specifications, coupled with the failure to anticipate a third party implementation, the CRTC, along with the involved industry stakeholders, did not produce a robust set of legislative or regulatory guidance.

However, despite granting iOptOut legitimacy, neither the Bell Canada administered DNCL nor the CRTC link to iOptOut's website or explain the role of iOptOut to consumers. iOptOut provides links to both organizations and explains the relationship between the lists. While never stated publicly, the lack of co-linking indicates the refusal of the CRTC to openly engage in collaboration with iOptOut. Shutting iOptOut out of 'official' websites results in less publicity for either the iOptOut service or the DNCL shortcomings.

The weak involvement of civil society or consumer organizations throughout the entire DNCL process led to a poor solution to the privacy problems raised by telemarketing. The iOptOut initiative is a direct response to this perceived weakness. As an example of an innovative NGO instrument, iOptOut offers a compelling solution to the issues of

Intrusion that the DNCL legislation and implementation fail to address. iOptOut also presents an innovative process which allows for the use of proxies by individuals to protect their privacy rights. This use of proxies may alleviate the capacity asymmetries between individuals and businesses. iOptOut is also an example of how a rival approach adopted and modeled by a civil society actor may compensate for information asymmetries that arise when business acts on behalf of government in carrying out a governance functions (as is the case with the CRTC approved DNCL approach).

In this chapter, we have observed how legislation can be ineffective as a result of problems arising during both its drafting and its implementation. Vulnerable to lobbying, political realities, market pressure, resource constraints and human oversight, legislative responses cannot be counted upon to provide a single shot solution. The DNCL example illustrates how a failure to recognize an articulated set of privacy problems results in a weak foundation. A weak process compounds, rather than addresses, these limitations.

There are several important observations revealed by examining the DNCL legislation and the technology decisions. First, there was a general misunderstanding, or conflicting understanding, of the value of private data and privacy protection requirements. For example, the data being collected by the National DNCL was viewed by the CRTC process as ‘only a phone number’, it was deemed not to be overly sensitive data.²³⁹ The privacy technology options were limited by the historical precedent, legislation and heavy influence of industry. In fact, the technology choice process occurred somewhat haphazardly as there was no process for technology choice discovery or decision or a

²³⁹ Do-Not-Call List Operations Working Group, *supra* note 179 at 45.

balancing of industry and consumer protection requirements. This led to failure to recognize the danger of Insecurity and Surveillance posed by telemarketing.

There were several process weaknesses including the lack of conceptual or technology PIAs to provide early guidance. The general lack of internal capacity at the CRTC to assess the privacy technology options and issues and the inability to take appropriate action left the CRTC dependant on external resources for legal and policy advice, RFP development and technology services. This dependence externalized expertise and lead to an over reliance on industry vendors and advocates agitating for specific industry solutions. The lack of technical capacity and externalization of technical expertise lead to an inability to take technical leadership positions that would require, promote and advance the deployment of innovative privacy enhancing architectures, business solutions and technologies.

The DNCL operations and technology decisions were primarily industry driven with a focus on increased profit maximization and decreased implication for telemarketers. There was no privacy technology innovation presented by industry at any point in the proposal process and there was no motivation provided to inspire innovation. The lack of privacy preserving architectures and technologies at the RFI stage limited the potential final technology requirements in the RFP. Due to the mandate for cost recovery and a lack of government funding there was little motivation for industry to undertake privacy innovation.

The privacy technology options were limited by the CMA historical precedent, legislative framework enacted and the heavy involvement of industry focused on profit. Poor consumer or civil society involvement limited the discussion of potential privacy problems identified and the range of potential privacy protections considered. There was no systematic attempt to tie operations and technology decisions to identified consumer privacy issues. It is therefore no surprise when the industry solution presented, selected and implemented represented a weak privacy solution. The failure of all major actors to foresee a third party response is indicative of a failure to design the DNCL within a comprehensive sustainable governance design.

The proliferation of telemarketing was only possible through an explosion of telecommunications and computerization within society. Any solution designed to address telemarketing must be integrated with and utilize the power of telecommunications technology. Unfortunately, governments and industry have a history of not choosing the most innovative privacy technology or demonstrating privacy technology leadership.²⁴⁰ Industry has not filled the privacy void with innovative or accessible solutions. The DNCL is an excellent example of how the government and its chosen industry partner failed to address the fundamental privacy issues and demonstrate technology leadership. A failure of appropriate technology design and operations both failed to mitigate against existing privacy problems and may have in turn exacerbated them.

²⁴⁰ Antonella Artuso, "New ID card threatens our privacy" *Toronto Sun* (21 October 2008), online: <<http://www.torontosun.com/news/canada/2008/10/21/7151421-sun.html>>.

In the final chapter, we will demonstrate how a sustainable governance approach may provide more effective consumer protection initiative.

Chapter Five: Sustainable Governance lessons for the DNCL

The argument of this thesis is twofold. First, in order to develop adequate privacy solutions there must be an appropriate understanding of the nature of the privacy problems at issue. Secondly, the development of *sustainable* privacy solutions require the balanced participation of all stakeholders utilizing a range of innovative institutions, instruments and processes.

Chapter two began by noting that there are many serious business practices that are impacting consumers. The exact nature of the activities and the long-term implications are not known. While there is no overwhelming consensus, many consumers have begun to assert that they feel their privacy has been invaded. Others have sacrificed privacy for convenience. The information technology revolution has brought a new dimension to the old problem of privacy. Traditional privacy approaches have limited effectiveness in the development of policy or legislation. Understanding privacy problems in a pluralistic, context-specific manner allows for realistic solutions to emerge. Solove's taxonomy of privacy was presented as a practical way to categorize privacy problems so that solutions can be developed.

Chapter three illustrated the traditional assumptions behind the roles that industry, individuals and government play in the general protection of personal privacy. Each actor has a set of motivations for involvement in the issue, various strengths and resources they

can leverage as well as assorted weaknesses that limit their effectiveness. The case was made that the three main actors are not individually capable of solving general consumer privacy problems. Kernaghan Webbs' notion of 'sustainable governance' was put forth as a better approach to addressing privacy problems. Sustainable governance incorporates concepts of reciprocally supporting collaborations that are knowingly and systematically designed to address an issue. Webb asserts the position that traditional governmental command and control models are limited and that there are a range of non-state actors that have an interest and capacity to address social problems. Recognizing the limits of traditional government and the potential of non-state actors, a sustainable governance approach would systematically develop and engage innovative actors, institutions, instruments and processes in collaborative problem solving and the governing of the public interest. This thesis argues that a sustainable governance approach which draws on the full range of actors, instruments, institutions and processes, in a mutually reinforcing manner, stands the greatest likelihood of effectively and efficiently protecting personal information over time.

Chapter four focused on the specific privacy issue of telemarketing. Using the taxonomy of privacy problems developed by Daniel Solove, it was argued that there are a number of 'privacy problems' raised by telemarketing and that overlooking these problems contributed to an inadequate DNCL solution. The failure to grasp the nature and importance of the privacy problems raised by telemarketing coupled with a failure to adopt an inclusive process resulted in flawed legislation and technology choices. These weaknesses led to the emergence of a third party solution called iOptOut.

This chapter will conclude by offering specific observations on how adopting a sustainable governance approach - including the use of innovative institutions, instruments and processes could improve the protection of privacy for individuals in the next generation DNCL. In particular, I will consider the ways in which innovations may contribute to a more sustainable approach to protect consumer privacy in the telemarketing context. Incorporating innovative NGO consultation processes, rule instrument innovations and institution innovations could substantially improve civil society engagement.

The first innovation to be considered is the creation of a more balanced consultation process that both empowers and includes civil society representatives. According to Webb, one of the primary principles of sustainable governance is the full participation of civil society. Despite having federal privacy legislation and a commissioner, Canada does not have a civil society advocacy organization exclusively dedicated to privacy issues. This means that in Canada privacy becomes ‘tacked onto’ or is merely a tangential issue for other advocacy organizations. In Canada, privacy advocacy has largely been conducted by the British Columbia Civil Liberties Association which has been involved over the years in issues such as video surveillance and national identification cards but was not involved in the DNCL. Similarly, while the Consumers’ Association of Canada was involved with the development of *PIPEDA*, it chose not to publicly comment on the DNCL.²⁴¹ Option Consommateurs is active in consumer

²⁴¹ Colin Bennett, *supra* note 137 at xxi-xxiii, 39, 45.

protection but operates primarily in French focused on Quebec consumer issues.²⁴² It has already been observed in the previous chapter how the Public Interest Advocacy Centre (PIAC) chose not to become as actively engaged in the DNCL process as it could have. There are no public interest technology advocacy organizations in Canada who are capable of intervening to promote innovative privacy technologies. I will argue below that a systematic inclusion of a robust privacy advocacy community could make specific improvements to the legislation, regulations and technology choices.

The government enjoys the benefit of utilizing a mature set of institutions and processes for the development, review and enactment of legislation. Almost all government actions include specific requirements and mandates for public consultation. Over the years, the Canadian government has made efforts to develop online citizen consultation processes and has developed one of the first government online web offerings. On its face, the CRTC currently has one of the most active and transparent public consultation processes in Canada. To its credit, that transparency allowed for the observation and documentation of the process of developing and implementing the DNCL legislation. Legislative hearings are open to the public, notices, submissions, and transcripts are available online free of charge.

There are several examples of process, institution and instrument innovations that could be incorporated into a *sustainable* DNCL governance process. These include innovation consultation and funding processes, establishing innovative privacy certification

²⁴² Option Consommateur, online: <<http://www.option-consommateurs.org/en/who/mission>>.

instruments and creating new privacy institutions that could continue effective consumer protection.

In order for government to adopt a sustainable governance approach, it must first recognize that there are multiple stakeholders involved in social issues who must be brought equally to the table. Business, civil society and consumer interests are not the same and should not be lumped together under a broad ‘public consultation’ umbrella. Consumer issues and business interests are often at direct odds with one another. Neither is there always consensus within civil society on issues. In the case of the DNCL, we observed how the charitable sector came into direct conflict with the consumer and privacy advocacy communities over their exemption from the DNCL. There is no current government requirement to provide a ‘balanced’ consultation between competing interests. Imposing such a formal requirement would objectively illustrate the competing interests and parties involved and provide a seating template for all consultations.

An example of an innovative consultation process is the Canadian Environmental Network (RCEN). The RCEN is provided both federal core and program funding to serve as the consultation hub between Environment Canada (and affiliated governmental partners) and more than 600 Canadian environmental groups. The organizations include a wide range of environmental issues from the atmosphere to toxins. The RCEN provides coordination, communication, research and networking services notably through their Delegate Selection Process. During the delegation selection process, RCEN and Environment Canada negotiate for equal stakeholder representation and provide capacity

support, including translation and simultaneous interpretation needs, and funding for NGO participation. The RCEN forms an independent delegate selection group who makes a delegate decision based on the pre-determined selection criteria. Selected delegates are supported by the RCEN and are sent information about the particulars and background of the consultation as well as coordinating opportunities for the selected delegates to exchange information prior to the consultation. This process enables the coordinated and funded participation of an extended range of appropriate NGOs in identified issues.²⁴³

The development of a similar model for privacy related consumer organizations would assist in the maturing of the consumer non-governmental movement. Currently, there is no centralized structure that supports the work of consumer NGOs. Groups must compete for limited project based funding and are dependent on limited internal expertise. Consumer groups in Canada must currently respond to a variety of topics. There is no consumer group solely dedicated to the issue of telemarketing. Neither are there specific NGOs to address issues of SPAM, internet regulations or biometrics, issues that are poised to be of central consumer concern. As such, there is no centralized body that is available to coordinate expertise or experience around privacy issues. While there are a few organizations in Canada capable of commenting on privacy issues, there are no non-government organizations that are able to address technology issues on an on-going basis. Several academic teams including Ron Dieberts' Citizen Lab at the Munk Centre for International Studies at the University of Toronto who uncovered international spyware

²⁴³ Canadian Environmental Network, "A Model Process for Delegate Selection", online: <http://www.cen-rce.org/eng/consultations/delegate_selection.html>.

activities²⁴⁴ and the Identity Trail project out of the University of Ottawa have emerged but there is no formal process by which academics can collaborate with either civil society organizations, industry or government.²⁴⁵

The second major obstacle that must be overcome to implement a sustainable governance approach is the recognition that there is a disproportionate level of capacity between businesses and civil society organizations. Industry has access to funds to operate and lobby in its own interest. While the CRTC may reimburse contributors for some expenses for specific consultation involvement, there is no federal core funding given to any privacy civil society organization. The lack of core funding means that there are no privacy organizations that could establish and provide their own independent institutional capacity for engaging on privacy issues on a consistent basis. The DNCL public record continually demonstrated that telemarketing industry was overwhelmingly involved in all aspects of the DNCL legislation and implementation. While there was a clear and available process for public involvement, civil society organizations in Canada were not substantively able to engage proportionally in this process. This must change in order for true collaboration to emerge.

Pippa Lawson, former CIPPIC director has publicly and repeatedly raised the issue of funding for NGO participation in stakeholder meetings. At a leading Asia Pacific Economic Cooperation (APEC) meeting to discuss the development of a privacy

²⁴⁴ Munk Centre for International Studies at the University of Toronto, "Press Conference / Webcast on Cyber Spy Network" (30 March 2009), online: <http://webapp.mcis.utoronto.ca/NewsDetail.aspx?newsid=544>.

²⁴⁵ On the Identity Trail, "On the Identity Trail: Our Investigation", online: <http://www.idtrail.org/content/view/12/34/>.

framework, she critiqued industry and government leaders for their failure to include civil society organizations from the outset, instead presenting them with results for comment.

The results, she points out, are inadequate.²⁴⁶ Lawson later stated:

It will be important, in our view, to ensure that the APEC assessment guidelines for both organisations and trustmarks meet our minimum standards. This will require a significant expenditure of time and expertise on the part of civil society representatives. If APEC is serious about consultation with civil society, it needs to address the question of funding for continued participation by informed consumer and privacy advocates in the APEC processes.²⁴⁷

The issue of NGO funding is not trivial. The value and role of an NGO is to be able to provide neutral third-party opinions to both government and businesses. Accepting funding from organizations that may in turn be the target of investigations or criticism impacts perceived neutrality. One way to increase revenues to NGOs would be to follow the example of the *Ontario Environmental Bill of Rights Act* that allows individual consumers and NGOs to sue companies for civil damages.²⁴⁸ Unfortunately, the courts are inaccessible for most individuals and currently inaccessible for NGOs in most circumstances.²⁴⁹

²⁴⁶ Pippa Lawson, "Stakeholder Roles in the APEC Pathfinder and Beyond: A Civil Society Perspective" Vancouver B.C (22-23 September 2007), online: <<http://www.cippic.ca/uploads/Stakeholder%20Roles%20in%20the%20APEC%20Pathfinder%20and%20Beyond.pdf>>.

²⁴⁷ Privacy International, "APEC Privacy Initiative" Report from representatives of civil society on meetings in Lima, Peru (18-22 February 2008), online: <[http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-561712](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-561712)>.

²⁴⁸ *Environmental Bill of Rights*, S.C. 1993, S.O. 1993, c. 28.

²⁴⁹ Jennifer Chandler, "The Epidemic of Lost and Stolen Data: Are Custodians of Data Liable for Breaches of Data Security" Techlaw Magazine (2008), online: <<http://www.scribd.com/doc/4710986/TECHLAW-Magazine>>.

Currently, the DNCL legislation and regulations allows for the levying of Administrative Monetary Penalties (AMP) for violators of the DNCL regulations. Currently the AMP monies will go into the coffers of the Government of Canada. Directing a portion of those penalties to an NGO with the mandate of overseeing the telemarketing industry would provide a dual incentive. NGOs would gain funding for catching violators and the individuals would be more motivated to be vigilant knowing that they are under increased scrutiny.

The DNCL legislation sets the AMPs at \$1,500 for individuals and \$15,000 for corporations per infraction. In theory, each time a listed number is contacted the companies can be fined for each number. On its face, these fines are substantial but it remains to be seen if they will be enforced to the fullest extent. Additionally, it would potentially be more innovative to have AMPs tied to the company profits so as to create a profit disincentive. For example, if a telemarketing company has profits of 10 million dollars a year and only has to pay a fine of 150,000, the fine could be considered a cost of doing business. However, if that company made 10 million dollars a year and had to pay a penalty of 15%, the cost would be 1.5 million dollars.

An example of an innovative NGO initiated rule instrument is a certification program developed by the Forest Stewardship Council (FSC). The FSC established principles, criteria, and standards that encompass economic, social, and environmental concerns. Recognized as the strongest international system governing sustainable forest management, the FSC makes the point to include a broad range of stakeholders with

differing perspectives on the forestry sector. There is a stringent process for obtaining certification and third party partners assess industry compliance.²⁵⁰

There are several ways this model could be adapted for the telemarketing industry.

In British Columbia there is provincial telemarketing legislation. According to this legislation, there is a requirement for all telemarketers to be registered with the province. There is an online search tool that can be used to look up licensed businesses.²⁵¹ There is no requirement in the DNCL that a company register or use its services. The requirement is that a person on the list not be contacted. The DNCL could have required all companies to be registered and pay a proportional fee for the development of more robust technology. Additionally, international companies who wanted to telemarket in Canada could be asked to put forward a bond to ensure that there would be a way to hold them accountable if a company was deemed to have violated the DNCL terms of use even though the company was beyond jurisdictional enforcement. Additionally, a consumer NGO could develop a certification and inspection system that would assess the privacy, telemarketing and data management practices of companies.

Finally, next generation telemarketing institutions could be envisioned. iOptOut was designed by Professor Michael Geist as an applied research project. Perhaps its future could illustrate the degree to which the DNCL process innovates around its operations. iOptOut could be adopted by a NGO with expertise in telemarketing consumer protection

²⁵⁰ Forestry Certification Council, "What is "certification"?", online:
<http://www.fscus.org/faqs/what_is_certification.php>.

²⁵¹ Business Practices and Consumer Protection Authority of British Columbia, "Licensee Search", online:
<http://www.bpcpa.ca/index.php?option=com_licensesearch&Itemid=138>.

and benefit from an institutional set of resources. A NGO operating iOptOut could receive a portion of the AMP or other civil redress from DNCL violators. Conversely, a DNCL review could recognize the flaws in the legislation and implementation and move to incorporate the functionality of iOptOut into a single, harmonized service.

There is also a potential for the use of technology to make systemic improvements to the DNCL. Partnering with academics and NGOs, an innovative DNCL operator could fund or conduct experiments to evaluate and monitor bad actors. For example, experimenters could create a series of ‘honey-pot’ phone numbers. The DNCL operator could include those numbers on the telemarketers’ lists. Telemarketers with lax practices or scammers could be traced, caught and fined. This is similar to planted bikes police use to catch bike thieves or radar traps for speeders. AMPs from DNCL violators could be set toward developing next generation privacy enhancing technologies that could be incorporated into the DNCL operation.

What a sustainable governance approach understands, and iOptOut illustrates, is that there is a legitimate role for creative tension between stakeholders. A recent study completed on privacy policy development addressed the issue of competing interests within corporations. While the process is cumbersome, the report indicates that companies who attempt to recognize the motivations and needs of each stakeholder will more likely be successful.²⁵² While collaboration is the goal, the reality is that initial consensus may not always be feasible. The ability of iOptOut to step outside the industry

²⁵² Cynthia Nickel et al. “The Driving Motivations of Stakeholders in the Delivery of Privacy by Enterprises” HP Laboratories (21 October 2008), online: <<http://www.hpl.hp.com/techreports/2008/HPL-2008-153.pdf>>.

dominated process and present a more privacy positive solution shames dominant actors and potentially motivates them to move far beyond their initial comfort zone.

Despite a general lack of resources and capacity, civil society has the ability to access the general public through the media. Similarly, while neither Option Consommateurs or PIAC were able to be very effective in the process that led to the initial implementation of the DNCL, their ability to raise concerns in the media helped highlight the issues.²⁵³ Media exposure was equally as important to the success of iOptOut. iOptOut was operational well before the DNCL launched. It was able to harness the media attention being generated and insert itself in the conversation. A conversation that continues in the media today.

The paper posits that the privacy protection models currently in place for the DNCL represent "first generation" governance approach. This approach could be improved through the full inclusion of civil society organizations and the identification and adoption of innovative and more robust institutions, instruments and processes. Under a sustainable governance approach, civil society organizations will be able to contribute to the protection of consumer privacy with the establishment of processes to ensure equitable participation, design instruments that increase capacity and incorporate their expertise as well as through the creation and funding of robust privacy institutions.

²⁵³ Public Interest Advocacy Centre, *supra* note 179.

Appendix A – CSA / PIPEDA Principles

1. Accountability – organizations are responsible for the information under their control and they must know designate a person in the organization is accountable for protecting personal information.
2. Identifying Purposes – organizations must identify why they want to collect, use or disclose personal information before the information is collected
3. Consent – organizations must obtain consent when they collect, use or disclose personal information.
4. Limiting Collection – organizations must only collect information for the purpose identified and that collection must be done by fair and lawful means.
5. Limiting Use, Disclosure and Retention – organizations must not use or disclose personal information for purposes other than those for which it was collected, and that information should only as long as necessary to fulfill its purposes.
6. Accuracy – organization must ensure that the personal information it holds is accurate, complete and up-to-date.
7. Safeguards – organizations must protect personal information by taking appropriate security measures.
8. Openness – organizations must have personal information policies that are clear, understandable and readily available.
9. Individual Access – organizations must allow individuals to access to their personal information and ask for corrections if necessary.
10. Challenging Compliance – individuals can complain about how an organization handles their personal information if they feel their privacy rights have not been respected.

Appendix B - Telemarketing Chronology in Canada²⁵⁴

1876	– telephone is invented
1950's	– first telemarketing campaigns initiated
1970's	– the term telemarketing was developed - referring to Bell Canada's telecommunication systems
1988	– CMA voluntary do not contact list established
March 2001	– Industry Canada began reviewing telemarketing rules
May 2004	– CRTC Issued Telecom Decision 2004-35
December 13, 2004	– First reading of Bill C-37 in Parliament
February 7, 2005	– Bill C-37 referred to House committee
April 13, 2005	– Bill C-37 goes before the House Committee
June 13, 2005	– House report issued
October 20, 2005	– Second reading in Parliament
October 24, 2005	– Third reading in Parliament
October 25, 2005	– First reading in Senate
November 2, 2005	– Second reading in Senate
November 22, 2005	– Senate Committee Report issued
November 25, 2005	– Bill C-37 receives Royal Assent
February 20, 2006	– CRTC public consultation commenced
March 21, 2006	– Consortium of interested parties formed
June 30, 2006	– Bill C-37 – Amended legislation came into Force
July 7, 2006	– DNCL RFI initiated
July 2006	– Individual Vender consultation sessions
August 1, 2006	– DOWG Reports
July 30, 2007	– DNCL RFP issued
December 21, 2007	– Contract awarded to Bell Canada
December 2007	– Development work begun

²⁵⁴ This chronology builds on the one found in Computing in Medicine Research Group Memorial University of Newfoundland, *supra* note 76 at 47.

- January 2008 – RFP for complaints investigator
- February 14, 2008 – CRTC issues RFP for a Complaints Investigator
- March 25, 2008 – No RFPs received for a Complaints Investigator
- March 2008 – iOptOut launched by Michael Geist
- April 2008 – iOptOut validity challenged by the Canadian Marketing Association and Canadian Bankers Association
- July 2008 – CRTC rejects CMA & CBA complaint and validates I Opt as a legitimate consumer opt-out instrument

- September 30, 2008 – DNC Launch – DNCL website overwhelmed with volume. iOptOut also experienced a registration spike
- October 20, 2008 – CRTC considers adjusting telemarketing rules for political telemarketing, ADADs and harmonization with provincial legislation

Reference List

Cases and Legislation

An Act to amend the Telecommunications Act, R.S.C. 2005 c. 50, online:
<<http://www.crtc.gc.ca/ENG/LEGAL/TELECOM.HTM>>.

Anti-Terrorism Act, 2002 c.41 1st Session, 37th Parliament, online:
<<http://laws.justice.gc.ca/en/ShowDoc/cs/A-11.7//20090408/en>>.

Canadian Charter of Rights and Freedoms, The Constitution Act, 1982, Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11., online:
<<http://www.canlii.org/en/ca/const/const1982.html>>.

Dell Computer Corp. v. Union des consommateurs, (2007) 2 S.C.R. 801, 2007 SCC 34.

Environmental Bill of Rights, 1993 S.O. 1993, Chapter 28, online: <http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_93e28_e.htm>.

Hunter v. Southam Inc., [1984] 2 S.C.R. 145, online:
<<http://scc.lexum.umontreal.ca/en/1984/1984rcs2-145/1984rcs2-145.html>>.

Katz v. United States, 389 U.S. 347 (1967).

Leduc v. Roman, [2009] CanLII 6838 (ON S.C.).

Lobbying Act, R.S.C. 1985, C. 44 (4th Supp.), s. 1; 2006, c. 9, s. 66.

Personal Information Protection and Electronic Documents Act (PIPEDA), 2000 c.5 2nd Session, 36th Parliament.

Privacy Act, R.S., 1985, c. P-21.

R. v. Patrick, 2009 SCC 17. [2009].

R. v. Tessling, 209 SCC 67. [2004] 3 S.C.R. 432.

Telecommunications Act, R.S.C. 1993, c. 38.

United States v. Jacobsen, [1984] 466 U.S. 109.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 [US PATRIOT ACT], Pub. L. 107-56, 272 Stat. 115 (2001), online: <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107>

Government Documents

Australia Communications and Media Authority, “Do Not Call Register – Complaints and investigations” (December 2008), online:

<http://www.acma.gov.au/webwr/_assets/main/lib310037/is154-dncr-complaints_and_investigations-consumer.pdf>.

Business Practices and Consumer Protection Authority of British Columbia, “Licensee Search”, online:

<http://www.bpcpa.ca/index.php?option=com_licensesearch&Itemid=138>.

Canadian Radio-television and Telecommunications Commission (CRTC) “Telecom Decision CRTC 2004-35” (21 May 2004), online:

<<http://www.crtc.gc.ca/eng/archive/2004/dt2004-35.htm>>.

Canadian Radio-television and Telecommunications Commission (CRTC) “Telecom Decision 2006-4” (20 February 2006), online:

<<http://crtc.gc.ca/eng/archive/2006/pt2006-4.pdf>>.

Canadian Radio-television and Telecommunications Commission (CRTC) “Telecom Public Notice 2007-48” (3 July 2007), online:

<<http://www.crtc.gc.ca/eng/archive/2007/dt2007-48.htm>>.

Canadian Radio-television and Telecommunications Commission (CRTC) Letter to the Canadian Marketing Association “Re: Do Not Call requests made through iOptOut.ca Reference # 392251” (27 June 2008), online:

<http://www.michaelgeist.ca/component/option,com_docman/task,doc_download/gid,19/>.

Canadian Radio-television and Telecommunications Commission (CRTC) “National DNCL Webinar Presentation” (24 September 2008), online: <<http://www.thecma.org/PublicUploads/228620NationalDNCLCMASeptember24.pdf>>.

Canadian Radio-television and Telecommunications Commission (CRTC) “Telecom Decision CRTC 2008-6-1 (20 October 2008), online:

<<http://www.crtc.gc.ca/eng/archive/2008/dt2008-6-1.htm>>.

Do-Not-Call List Operations Working Group, “Report to the CRTC – Non-Consensus Report” (26 July 2006), online: <<http://www.crtc.gc.ca/public/cisc/do/DORE0001b.doc>>.

Do-Not-Call List Operations Working Group, “Report to the CRTC –Consensus Report” (26 July 2006), online: <http://www.crtc.gc.ca/public/cisc/dc/Con_Rpt-1.doc>.

Government of Canada, "ICT and Canada: The Future Is Here", online:
<<http://investincanada.gc.ca/eng/publications/ict-canada.aspx>>.

House of Commons Standing Committee on Industry, Natural Resources, Science and Technology, Evidence, 38th Parliament, 1st Session.

House of Commons Standing Committee on Industry, Natural Resources, Science and Technology, "Sixth Report" 38th Parliament, 1st Session (8 June 2005), online:
<<http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=1916112&Language=E&Mode=1&Parl=38&Ses=1>>.

House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) Evidence, 39th Parliament, 1st Session.

House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) "Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics" 39th Parliament, 1st Session (May 2006), online:
<<http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=2891060&Language=E&Mode=1&Parl=39&Ses=1&File=5>>.

House of Commons "Government Response to the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics: Statutory Review of the Personal Information Protection and Electronic Documents Act" 39th Parliament, 1st Session (2006), online:
<<http://www2.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&Parl=39&Ses=1&DocId=3077726&File=0>>.

House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) Evidence, 39th Parliament, 2nd Session.

Human Resources and Skills Development Canada, "An Evaluation of the Sectoral Involvement in Departmental Policy Development (SIDPD)" (March 2004), online:
<<http://www.hrsdc.gc.ca/eng/cs/sp/sdc/evaluation/sp-ah214e/page03.shtml>>.

Industry Canada, "Minister of Industry Tables Legislation for National Do Not Call List" (13 December 2004), online: <<http://www.ic.gc.ca/eic/site/ic1.nsf/eng/02336.html>>.

National Do Not Call List. "Frequently Asked Questions", online: <https://www.lnntedncl.gc.ca/faqs-eng#an_link09>.

Public Safety Canada, "Advice for consumers identity theft", online:
<<http://www.publicsafety.gc.ca/prg/le/bs/consumers-en.asp>>.

Office of the Commissioner of Lobbying of Canada, "Annual Report 2007-2008", online:
<<http://www.ocl-cal.gc.ca/eic/site/lobbyist-lobbyiste1.nsf/eng/nx00319.html#s11>>.

Office of Consumer Affairs, "Consumer Trends Report" Government of Canada. (20 September 2007), online: <<http://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca02096.html#tlc>>.

Office of the Information and Privacy Commissioner of Ontario "Identity Theft Revisited: Security is Not Enough" (1 September 2005), online: <<http://www.ipc.on.ca/images/Resources/idtheft-revisit.pdf>>.

Office of the Privacy Commissioner of Canada, "Substantially Similar Provincial Legislation", online: <http://www.privcom.gc.ca/legislation/02_06_01_e.asp>.

Office of the Privacy Commissioner of Canada, "Privacy in the Workplace", online: <http://www.privcom.gc.ca/fs-fi/02_05_d_17_e.asp>.

Office of the Privacy Commissioner of Canada, "Statutory Review of the Personal Information Protection and Electronic Documents Act Background Information on the OPC's Consultation" (27 November 2006), online: <http://www.privcom.gc.ca/parl/2006/sub_061127_e.asp>.

Office of the Privacy Commissioner of Canada, "Privacy Commissioner Response to PIAC Proposal" (12 January 2004), online: <http://www.piac.ca/privacy/privacy_commissioner_response_to_piac_proposal>.

Office of the Privacy Commissioner of Canada, "Letter to Air Canada's Manager of Privacy Compliance, Erik Grados" News Release (20 March 2002), online: <http://www.privcom.gc.ca/media/nr-c/02_05_b_020320_e.asp>.

Office of the Privacy Commissioner of Canada, "Privacy in the Marketplace Remarks for CMA Regulatory Affairs Conference" (Public Address by Jennifer Stoddart, 14 September 2006), online: <http://www.privcom.gc.ca/speech/2006/sp-d_060914_e.asp>.

Standing Senate Committee on Transport and Communications, "Ninth Report" 38th Parliament, 1st Session Government of Canada (22 November 2005), online: <<http://www.parl.gc.ca/38/1/parlbus/commbus/senate/com-e/tran-e/rep-e/rep09nov05-e.htm>>.

Statistics Canada, "Quarterly Telecommunications Statistics 4th Quarter, 2005" Science, Innovation and Electronic Information Division Vol. 29, no.4 (May 2006), online: <<http://dsp-psd.pwgsc.gc.ca/Collection-R/Statcan/56-002-XIB/56-002-XIE2005004.pdf>>.

Treasury Board of Canada Secretariat, "Privacy Matters: The Federal Strategy to Address Concerns About the USA PATRIOT Act and Transborder Data Flows" (29 March 2006), online: <http://www.tbs-sct.gc.ca/pubs_pol/gospubs/tbm_128/pm-prp/pm-prp01-eng.asp>.

Treasury Board of Canada Secretariat, "Privacy Impact Assessment Policy" (2 May 2002), online: <<http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12450§ion=text#cha3>>.

United States, Federal Communications Commission, "Something to Share" (21 November 2005), online: <<http://www.fcc.gov/omd/history/internet/something2share.html>>.

United States, Federal Trade Commission, "Q&A: The National Do Not Call Registry" (July 2008), online: <<http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt107.shtm>>.

Secondary Sources

"5 Most Viral Video Youtube Collection Watch Online" (5 April 2009), online: <<http://current-news-results-notice.blogspot.com/2009/04/5-most-viral-video-youtube-collection.html>>.

Albrecht, Katherine. "Supermarket Cards: The Tip of the Retail Surveillance Iceberg" online: (Summer 2002) Volume 79, Issue 4. *Denver University Law Review*, <<http://www.spychips.com/documents/Albrecht-Denver-Law.pdf>>.

Anderson, Ross. "Why Information Security Is Hard - An Economic Perspective" (Computer Security Applications Conference, 2001), online: <<http://www.cl.cam.ac.uk/~rja14/Papers/econ.pdf>>.

Artuso, Antonella. "New ID card threatens our privacy" *Toronto Sun* (21 October 2008), online: <<http://www.torontosun.com/news/canada/2008/10/21/7151421-sun.html>>.

Bell Canada. "Call Privacy", online: <http://www.bell.ca/support/PrsCSrvPns_STSHelp_Details_CallPrv.page>.

Bennett, Colin. *The Privacy Advocates: Resisting the Spread of Surveillance* (Cambridge: MIT Press, 2008).

Bennett, Colin and Charles Raab. *The Governance of Privacy: Policy Instruments in Global Perspective*. (Cambridge: MIT Press, 2003).

Borking, John. Oral remarks at the 21st International Conference on Privacy and Personal Data Protection, Hong Kong, China (September 1999).

Butler, Don. "Part II: Devil in the details when it comes to social sorting, you are what you eat, buy, surf, post" *Ottawa Citizen* (5 February 2009), online: <<http://www.ottawacitizen.com/Business/Part+Devil+details/1232337/story.html>>.

Call for Action. "Do Predictive Dialers Violate Rules?", online:
<<http://www.callforaction.org/tips/detail.asp?id=240>>.

Cameron, Kim. "Introduction to the Laws of Identity" *Kim Cameron's Weblog* (8 January 2006), online: <<http://www.identityblog.com/?p=354>>.

Canadian Bankers Association. "Submission of the Canadian Bankers Association CRTC File: 8662-C131-200408543" (07 September 2004), online:
<<http://www.crtc.gc.ca/public/partvii/2004/8662/cba/040907.zip>>.

Canadian Broadcasting Corporation (CBC) News. "Patriot Act seen as threat to Canadians' privacy" *CBC News* (20 June 2006), online:
<<http://www.cbc.ca/canada/story/2006/06/20/privacy-report.html>>.

Canadian Broadcasting Corporation (CBC) News. "Due diligence: The growing problem of mortgage fraud" *CBC News* (9 November 2006), online:
<<http://www.cbc.ca/news/background/mortgage-fraud>>.

Canadian Broadcasting Corporation (CBC) News. "1 in 6 Canadians hit by identity theft, survey suggests" *CBC News* (1 March 2007), online:
<<http://www.cbc.ca/consumer/story/2007/03/01/identify-fraud.html>>.

Canadian Broadcasting Corporation (CBC) News. "Do-not-call list" *CBC News* (30 September 2008), online: <<http://www.cbc.ca/news/background/telemarketing>>.

Canadian Broadcasting Corporation (CBC) News. "Thousands call to complain about do-not-call list" *CBC News* (27 November 2008), online:
<<http://www.cbc.ca/consumer/story/2008/11/27/calling.html>>.

Canadian Broadcasting Corporation (CBC) News. "80% of Canadians getting fewer telemarketing calls: survey" *CBC News* (9 March 2009), online:
<<http://www.cbc.ca/consumer/story/2009/03/09/no-call-canada.html>>.

Canadian Environmental Network. "A Model Process for Delegate Selection", online:
<http://www.cen-rce.org/eng/consultations/delegate_selection.html>.

Canadian Internet Policy and Public Interest Clinic (CIPPIC). "Lawful Access: Police Surveillance", online: <<http://www.cippic.ca/lawful-access/#LA21>>.

Canadian Internet Policy and Public Interest Clinic (CIPPIC). "Compliance with Canadian Data Protection Laws: Are Retailers Measuring up?" (April 2006), online:
<[http://www.cippic.ca/documents/bulletins/compliance_report_06-07-06_\(color\)_cover-english\).pdf](http://www.cippic.ca/documents/bulletins/compliance_report_06-07-06_(color)_cover-english).pdf)>.

Canadian Internet Policy and Public Interest Clinic (CIPPIC). "On the Data Trail: How detailed information about you ends up in the hands of organizations with whom you

have no relationship” (May 2006), online: <<http://www.cippic.ca/documents/May1-06/DatabrokerReport.pdf>>.

Canadian Marketing Association. “Measuring the Return on Investment in the Canadian Marketing Association”, online: <<http://www.thecma.org/PublicUploads/223585MembershipInformation.pdf>>.

Canadian Marketing Association. “Letter to CRTC Re: Telecom Public Notice CRTC 2006-4” (27 March 2006), online: <http://www.crtc.gc.ca/public/partvii/2006/8665/c12_200601626/606961.pdf>.

The Canadian Marketing Association. “Operation Integrity”, online: <<http://www.thecma.org/?WCE=C=47|K=224219>>.

Canadian Resource Centre for Victims of Crime. “Brief to the Standing Committee on Access to Information, Privacy and Ethics Re: PIPEDA Review” (13 February 2007), online: <<http://www.crcvc.ca/docs/PIPEDA.BRIEF.pdf>>.

Cate, Fred. *Privacy in Perspective*. (Washington DC: The AEI Press, 2001)
Children’s Aid Society of Simcoe County, “History”, online: <<http://www.simcoecas.com/en/aboutus/history.asp>>.

Chandler, Jennifer. “The Epidemic of Lost and Stolen Data: Are Custodians of Data Liable for Breaches of Data Security” *Techlaw Magazine* (2008), online: <<http://www.scribd.com/doc/4710986/TECHLAW-Magazine>>.

Children’s Aid Society of Simcoe County. “History”, online: <<http://www.simcoecas.com/en/aboutus/history.asp>>.

Christensen, Dan. “Major Information Brokers Face Class Action for Invasion of Privacy” *LAW.COM* (24 June 2003), online: <<http://www.law.com/jsp/article.jsp?id=1056139884864>>.

Clark, Roger. “Business Cases for Privacy-Enhancing Technologies” in Subramanian R., ed. *Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions* (Hershey, PA: IDEA Group, 2008), online: <<http://www.rogerclarke.com/EC/PETsBusCase.html>>.

Commission on Global Governance. *Our Global Neighbourhood* (Oxford: Oxford University Press, 1995).

Computing in Medicine Research Group Memorial University of Newfoundland. “Private / Public Sharing of Personal Information: Lessons from the health care sector” Office of the Privacy Commissioner of Canada Contributions Program (March 2008).

Consumers' Association of Canada. "Telecommunications", online:
<<http://www.consumer.ca/1530>>.

Contact Centre Canada. "Frequently Asked Questions", online:
<<http://www.contactcentrecanada.ca/en/about-ccc/faq.aspx>>.

Corporate Solutions Consulting. "Fair Processing Notifications: Current Effectiveness and Opportunities for Improvement" (22 January 2007), online:
http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/ic_final_report_version_1.1_final.pdf>.

Direct Marketing Association. "Contact Centres and Telemarketing", online:
<<http://www.dma.org.uk/sectors/cct-introduction.asp>>.

EKOS Research Associates. "Canadian Businesses and Privacy-Related Issues" Office of the Privacy Commissioner of Canada (March 2007), online:
<http://www.privcom.gc.ca/information/survey/2007/ekos_2007_01_e.asp#summary>.

EPIC. "The USA PATRIOT Act", online: <<http://epic.org/privacy/terrorism/usapatriot/>>.

Espiner, Tom. "U.K.'s Home Office admits to database breaches" *CNET News* (31 August 2006), online: <http://news.cnet.com/U.K.s-Home-Office-admits-to-database-breaches/2100-1029_3-6111358.html?tag=mncol>.

Espiner, Tom. "U.K. government reveals its 'biggest privacy disaster'" *CNET News* (21 November 2007), online: <http://news.cnet.com/U.K.-government-reveals-its-biggest-privacy-disaster/2100-1029_3-6219772.html>.

Facebook Press release. "Leading Websites Offer Facebook Beacon for Social Distribution" (6 November 2007), online:
<<http://www.facebook.com/press/releases.php?p=9166>>.

"Facebook Bill of Rights and Responsibilities", online:
<<http://www.facebook.com/group.php?gid=69048030774>>.

Forestry Certification Council. "What is "certification"?", online:
<http://www.fscus.org/faqs/what_is_certification.php>.

Fournier, Danielle. "Datagate- The 21st Century Scandal?" *Monitor Magazine*, online:
<<http://www.monitortoday.com/Datagate.pdf>>.

Fusepoint News Release. "Fusepoint Data Confidence Survey" (24 October 2007), online:
<http://www.fusepoint.com/english/downloads/FP_Survey_Release_Oct_07_ENG.pdf>.

Geist, Michael. "Do-not-call faces challenges" *The Star* (9 October 2008), online: <<http://www.thestar.com/columnists/article/410819>>.

Geist, Michael. "Canada's Do-Not-Hesitate-To-Call List" (11 September 2005), online: <<http://www.michaelgeist.ca/index.php?option=content&task=view&id=950>>.

Geist, Michael. "Lawless Canada Emerging as a Spam Haven" (1 December 2008), online: <<http://www.michaelgeist.ca/content/view/3552/159/>>.

Geist, Michael. "CMA and MRIA Recommend Against Respecting iOptOut Requests" (8 April), online: <<http://www.michaelgeist.ca/content/view/2820/135/>>.

Haselton, Bennett. "Janet Garrow, Bellevue District Court", online: <<http://www.judgejokes.com/janet-garrow.html>>.

Haselton, Bennett. "Anti-Spam Suits and Booby-Trapped Motions" (18 April 2007), online: <<http://yro.slashdot.org/article.pl?sid=07/04/18/1247229>>.

Harry, Mikel & Richard Schroeder. *Six Sigma: The Breakthrough Management Strategy Revolutionizing the World's Top Corporations* (New York: Doubleday Business, 1999).

Head, Tom. "Privacy After 9/11" *About.com*, online: <<http://civilliberty.about.com/od/waronterror/ig/War-on-Terror-101/Privacy-After-9-11.htm>>.

Hosein, Gus. "International Co-operation as a Promise and a Threat" in *Cybercrime and Jurisdiction: A Global Survey*, Bert-Japp Koops and Susan W. Brenner (The Hague: TMC Asser Press, 2006), online: <[http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-543297](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-543297)>.

Hughes Anthony, Nancy. "Banks are in favour of national Do Not Call list" *The Vancouver Sun* (8 August 2008), online: <<http://www2.canada.com/vancouversun/news/letters/story.html?id=0b7dbacf-ef55-4b58-b5f2-619904a891d4>>.

Hyndman, Rob. "Do-Not-Hesitate-to-Call is in the Senate" (5 November 2005), online: <<http://www.robhyndman.com/2005/11/05/do-not-hesitate-to-call-is-in-the-senate/>>.

itWorldCanada. "The 8 most dangerous consumer technologies" (6 September 2007), online: <<http://www.itworldcanada.com/a/The-good-the-bad-and-the-ugly/69d9da03-0842-4840-8526-1ba2a01b198e.html>>.

International Security, Trust & Privacy Alliance. "Privacy Framework" Version 1.1 (2002), online: <<http://www.istpa.org/pdfs/ISTPAPrivacyFrameworkV1.1.pdf>>.

iOptOut. "Do-Not-Call Registry Early Glitches" (2 October 2008), online:
<http://ioptout.ca/index.php?option=com_multisite&Itemid=18>.

iOptOut. "Enforcing Your Opt Out", online:
<https://ioptout.ca/index.php?option=com_content&task=view&id=9&Itemid=20>.

Jackson, Brian. "Privacy controversy mars Google Apps rollout at Canadian university" *itbusiness.ca* (11 July 2008), online:
<<http://www.itbusiness.ca/it/client/en/Home/News.asp?id=50660&PageMem=3>>.

Kerr, Ian, Max Binnie & Cynthia Aoki. "Tessling on my Brain: The Future of Lie Detection and Brain Privacy in the Criminal Justice System", *Canadian Journal of Criminology and Criminal Justice*, (Forthcoming 2008), online:
<http://iankerr.ca/images/stories/tessling_on_my_brain.pdf>.

Lawson, Pippa. "Stakeholder Roles in the APEC Pathfinder and Beyond: A Civil Society Perspective" Vancouver B.C (22-23 September 2007), online:
<<http://www.cippic.ca/uploads/Stakeholder%20Roles%20in%20the%20APEC%20Pathfinder%20and%20Beyond.pdf>>.

Leise, Cindy. "When MLK came to Oberlin", *The Chronicle-Telegram* (21 January, 2008), online: <<http://www.chroniclet.com/2008/01/21/when-mlk-came-to-oberlin>>.

Lemos, Robert. "MasterCard warns of massive credit-card breach", *SecurityFocus* (17 June 2005), online: <<http://www.securityfocus.com/news/11219>>.

Munk Centre for International Studies at the University of Toronto. "Press Conference / Webcast on Cyber Spy Network" (30 March 2009), online:
<<http://webapp.mcis.utoronto.ca/NewsDetail.aspx?newsid=544>>.

Long, Murray. *PrivacyScan* (1 October 2007).

Long, Murray. *PrivacyScan* (29 September 2008).

Marcotee Stamer, Cynthia. "Texas AG suit Against Radio Shack for Alleged Violation of 2005 Texas Identity Theft Law" *Risk Management and Compliance E-News* (10 April 2007), online:
<<http://www.cynthiastamer.com/documents/alerts/20070409%20Identity%20Theft%20Updates.pdf>>.

McDonald, Aleecia and Lorrie Faith Cranor. "The Cost of Reading Privacy Policies" (Paper Presented to the Telecommunications Policy Research Conference, 26 September 2008), online: <<http://www.scribd.com/doc/7550344/Cost-of-Reading-Privacy-Policies>>.

McMillan, Robert. "Half a million database servers 'have no firewall'" *IDG News Service* (14 November 2007), online:

<<http://www.computerworlduk.com/management/security/data-control/news/index.cfm?newsid=6198>>.

Market Research and Intelligence Association. "Telemarketing Do-Not-Call Registry Becomes Law .Major Win For Survey Research" (25 November 2005), online: <<http://www.mria-arim.ca/NEWS/Telemarketing.asp>>.

Market Research and Intelligence Association. "MRIA launches the world's first Charter of Respondent Rights" (3 October 2006), online: <<http://www.mria-arim.ca/STANDARDS/RespondentRights.asp>>.

Market Research and Intelligence Association. "MRIA Member Advisory On iOptOut.ca" (2 August 2007), online: <<http://www.mria-arim.ca/INDMEMBERSONLY/CorpAdvisory-08-02-07NP.asp>>.

May, Kathryn. "Government to replace \$1B online service 'boondoggle'" *Ottawa Citizen* (17 October 2008), online: <<http://www2.canada.com/ottawacitizen/news/story.html?id=53c07185-f270-4fca-b660-6b382bae2b16>>.

Mills, Elinor. "Payment processor Heartland reports breach" *CNET News* (20 January 2009), online: <http://news.cnet.com/8301-1009_3-10146275-83.html>.

Elinor Mills. "User data stolen from job site Monster" *CNET News* (26 January 2009), online: <http://news.cnet.com/8301-1009_3-10149884-83.html>.

Moore, David, et al. "Inside the Slammer Worm" *IEEE Security and Privacy Magazine* (July/August 2003), online: <<http://www.cs.ucsd.edu/~savage/papers/IEEEESP03.pdf>>.

NEXT. "How DigiCash Blew Everything" (January 1999), online: <<http://jya.com/digicrash.htm>>.

Nickel, Cynthia, et al. "The Driving Motivations of Stakeholders in the Delivery of Privacy by Enterprises" HP Laboratories (21 October 2008), online: <<http://www.hpl.hp.com/techreports/2008/HPL-2008-153.pdf>>.

Ponemon Institute. "Consumers' Report Card on Data Breach Notification" (15 April 2008).

On the Identity Trail. "On the Identity Trail: Our Investigation", online: <<http://www.idtrail.org/content/view/12/34/>>.

Option Consommateur. online: <<http://www.option-consommateurs.org/en/who/mission>>.

Option Consommateurs. "Right of Access to Personal Information: The Key to the Right of Privacy" (2006), online: <<http://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca02075.html#projf>>.

PCtools. "Email insecurity highlighted by Lord West" (26 March 2009), online: <http://www.pctools.com/industry-news/article/email_insecurity_highlighted_by_lord_west-19092984/>.

Phone Busters. "Recognize it", online: <<http://www.phonebusters.com/english/recognizeit.html>>.

Phone Busters. "Monthly Summary Report", online: <http://www.phonebusters.com/english/documents/MonthlyStats_000.pdf>.

Privacy Corps. "Caller ID Information", online: <<http://www.privacycorps.com./pages/caller-id-information.htm>>.

Privacy Rights Clearinghouse. "A Chronology of Data Breaches" (April 2009), online: <<http://www.privacyrights.org/ar/ChronDataBreaches.htm>>.

Privacy International. "APEC Privacy Initiative" Report from representatives of civil society on meetings in Lima, Peru (18-22 February 2008), online: <[http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-561712](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-561712)>.

Public Interest Advocacy Centre. "Letter to Privacy Commissioner of Canada" (18 December 2003), online: <http://www.piac.ca/privacy/letter_to_privacy_commissioner_of_canada_1/>.

Public Interest Advocacy Centre. "Do-not-call registry: Junk phone calls are down" (10 February 2009), online: <http://www.piac.ca/other/public_interest_news_government_safeguards_air_canada_fuel_fee_cibc_470_752_clients_best_toys_and_worst_of_toys_webkinz_and_neopets_bank_wal_mart_online_banking_bdus_sms_spam/>.

Public Safety Canada. "Advice for Consumers Identity theft" (03 May 2008), online: <<http://www.publicsafety.gc.ca/prg/le/bs/consumers-en.asp>>.

Raab, Charles. "From Balancing to Steering: New Directions for Data Protection", in Colin Bennett and Rebecca Grant, *Visions of privacy; policy choices for the digital age*. (Toronto: University of Toronto Press, 1998).

Rabin, Mathew. "A Perspective on Psychology and Economics" (Working Paper No. E02-313 Department of Economics, University of California, February 2002), online: <<http://repositories.cdlib.org/cgi/viewcontent.cgi?article=1003&context=iber/econ>>.

Ragan, Steve. "Company privacy traded for candy" *The Tech Herald* (17 April 2008),

online: <<http://www.thetechherald.com/article.php/200816/737/Company-privacy-traded-for-candy/>>.

Read, Brendan. "Canada: Third Party Do Not Call Exemption Collection OK" *Contact Center Solutions* (11 August 2008), online: <<http://callcenterinfo.tmcnet.com/analysis/articles/36571-canada-third-party-not-call-exemption-collection-ok.htm>>.

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

Roy Morgan Research. "Privacy and the Community" for the Australian Office of the Federal Privacy Commissioner (July 2001), online: <<http://www.privacy.gov.au/publications/rcommunity.html#1>>.

Scheier, Robert L. "Your data's less safe today than two years ago" *Computerworld*, online: <<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9031104&pageNumber=4>>.

Schmidt, Sarah. "Glitches mark launch of 'do-not-call' registry" *Canwest News Service* (30 September 2008), online: <<http://www.financialpost.com/news-sectors/story.html?id=851194>>.

Schick, Shane. "Canadian businesses stumbling over privacy compliance" *Computerworld* (25 July 2007), online: <<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9027951>>.

Shapira, Ian. "When Young Teachers Go Wild on the Web Public Profiles Raise Questions of Propriety and Privacy" *Washington Post* (28 April 2008) Page A01, online: <<http://www.washingtonpost.com/wp-yn/content/article/2008/04/27/AR2008042702213.html>>.

Sigma Assistel. "Cross-Canada survey on Identity Theft" (13 June 2007), online: <<http://www.assistel.com/NR/rdonlyres/0DA419C3-156E-4EEE-93C6-3902C3A0FD48/0/PressRelease.pdf>>.

Skelton, Chad. "Another B.C. NDP candidate resigns after marijuana video surfaces" *Vancouver Sun* (19 September 2008), online: <<http://www2.canada.com/vancouvernews/story.html?id=a61b51a4-bace-4fef-8feb-814d67e12b61>>.

Smith, Julie. "Facebook Growth Continuing, Surpasses 150 Million Monthly Active Users" *Inside Facebook* (7 January 2009), online:

<<http://www.insidefacebook.com/2009/01/07/facebook-growth-continuing-surpasses-150-million-monthly-active-users/>>.

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

Sproule, Susan & Norm Archer. "Measuring Identity Theft in Canada: 2006 Consumer Survey - Working Paper #21" (2006), online: <<http://www.merc-mcmaster.ca/working-papers/measuring-identity-theft-in-canada-2006-consumer-survey/>>.

Stalder, Felix. "The Voiding of Privacy" online: (August 2002) No.2 Sociological Research Online, <http://felix.openflows.com/html/FS_Voiding_of_privacy.pdf>.

Steeves, Val. "Legal and Policy Approaches to Identity Theft" ORNEC Identity Theft Research Project Workshop II University of Ottawa (13 October 2006), online: <www.rileyis.com/seminars/feb07/Vsteeves_feb_2007.ppt>.

Stone, Brad. "Our Paradoxical Attitudes Toward Privacy" *The New York Times* (2 July 2008), online: <<http://bits.blogs.nytimes.com/2008/07/02/our-paradoxical-attitudes-towards-privacy/?th&emc=th>>.

Symantec. "Symantec Reports Rise in Data Theft, Data Leakage, and Targeted Attacks Leading to Hackers' Financial Gain" (19 March 2007), online: <http://www.symantec.com/about/news/release/article.jsp?prid=20070319_01>.

The London School of Economics Centre for Civil Society. "What is civil society?" (4 March 2004), online: <http://www.lse.ac.uk/collections/CCS/what_is_civil_society.htm>

TruEffect Corporate Website. online: <<http://www.trueeffect.com>>.

UPI.COM. "1-in-10 Canadians hit by Web ID theft" (22 October 2008), online: <http://www.upi.com/Top_News/2008/10/22/1-in-10-Canadians-hit-by-Web-ID-theft/UPI-37041224679643/>.

Visa. "PCI Compliance Continued to Grow in 2007", online: <<http://www.corporate.visa.com/md/nr/press753.jsp>>.

Wappel, Tom. "Oral Comments" (CPO Roundtable, 6 March 2007).

Warren, Samuel & Louis Brandeis. "The Right to Privacy" 4 *Harvard Law Review* 193 (1890).

Webb, Kernaghan. "Sustainable Governance in the Twenty-First Century: Moving Beyond Instrument Choice" in *Designing Government From Instruments to Governance* (Montreal: McGill-Queen's University Press, 2005).

Webb, Kernaghan. "Government, Private Regulation, and the Role of the Market," in Michael MacNeil et al, *Law Regulation and Governance* (Toronto: Oxford University Press, 2002).

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