uOttawa

L'Université canadienne
Canada's university

t

FACULTÉ DES ÉTUDES SUPÉRIEURES ET POSTOCTORALES

uOttawa

L'Université canadienne
Canada's university

FACULTY OF GRADUATE AND POSDOCTORAL STUDIES

Karl Klockars
AUTEUR DE LA THÈSE / AUTHOR OF THESIS

M.A. (Criminology)
GRADE / DEGREE

Department of Criminology
FACULTÉ, ÉCOLE, DÉPARTEMENT / FACULTY, SCHOOL, DEPARTMENT

Governing the E-subject Through Identity Theft Discoures

TITRE DE LA THÈSE / TITLE OF THESIS

Valerie Steeves
DIRECTEUR (DIRECTRICE) DE LA THÈSE / THESIS SUPERVISOR

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

Martin Dufresne

Bastien Quirion

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

GOVERNING THE E-SUBJECT THROUGH IDENTITY THEFT DISCOURSES

KARL KLOCKARS
SUPERVISING PROFESSOR: DR. VALERIE STEEVES

A THESIS SUBMITTED TO THE FACULTY OF GRADUATE AND POSTDOCTORAL STUDIES IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE MASTER OF ARTS, CRIMINOLOGY

DEPARTMENT OF CRIMINOLOGY

Your file Votre référence
ISBN: 978-0-494-79682-5
Our file Notre référence
ISBN: 978-0-494-79682-5

ABSTRACT

This study explores the social construction of identity theft, including its meanings, risk factors, specific causes and accompanying solutions, articulated in policy documents published by the Consumer Measures Committee (a sub-committee of Industry Canada) and the Royal Bank of Canada. A qualitative analysis of the documents indicates that identity theft is predominately constructed within the documents as an individualized consumer concern. This is in keeping with the shift to neoliberalism identified by Monahan (2009) and Caeton (2007). Within this, individuals are constructed as buying into the electronic marketplace, aligning their own motivations with larger political and economic objectives, while trusting in the advice of experts to overcome manageable risks.

ACKNOWLEDGEMENTS

I would like to acknowledge and extend my heartfelt gratitude to the following persons who have made the completion of this study possible:

My supervising professor, Dr. Valerie Steeves, for her vital knowledge, patience, guidance and constant reassurance. It is difficult to overstate my appreciation for her and her efforts to help me see through the data for what it is. I would have been lost without her.

To the University of Ottawa staff and professors who helped me gain a sense of direction. I am especially grateful to Ron Melchers for pushing me during early morning seminars, Holly Johnson for reacquainting me with advanced research methods and Chris Bruckert for bringing Foucault's madness to an acceptable level.

To the local baristas at Starbucks, whose dispensing of legal addictive stimulants helped keep me writing with vigor and those who rejoiced with me in the wonder that is caffeine.

To my friends who were always there when I needed them, academically or socially.

To one woman in particular in whom I have found all I was ever looking for in a partner and best friend. She has opened my world to possibilities I never knew existed.

To my sister for always being able to make me smile and laugh even during tough times. Her constant love I always cherish.

To my parents. They bore me, raised me, taught me, and loved me. All that I am and all that I will ever be, I owe to my family.

And to God, in whom all things are made possible.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

Introduction

"Technology is neither *good* nor *bad*, nor even *neutral*. Technology is one part of the complex of relationships that people form with each other and the world around them; it simply cannot be understood outside of that concept" – Samuel Collins (unknown)

Identity theft (IDT) is allegedly one of the primary risks consumers and users face today in the digital marketplace. It is a cross-cutting crime that implicates consumer protection, market efficiency, policy approaches and protection efforts, and at the same time, touches upon the responsibilities of the public and private sector (CMC, 2007). It is also a crime garnering increased attention from academia, the media, policymakers and the public, fuelled in part by a growing body of statistical evidence that underscores its marked growth since the mid-1990s. Numerous agencies have offered statistics on the prevalence of IDT; however, Gordon et al. (2004:9) found that the collection of data from so many decentralized and distinct sources is, in some ways, piecemeal and, in other ways, duplicative. However flawed, those pieces have been assembled into a bigger picture of IDT which can now claim to be the fastest growing crime in North America (Henderson, 2005), growing at a rate of 30% per year in some areas (Lacey & Cuganesan, 2004). Elsewhere, it has been called the "quintessential crime of the information age" (Kahn & Roberds, 2007) and the "most prevalent financial crime" today (White & Fisher, 2008: 3).

Koops et al. (2009) claim that, despite its historical roots, IDT has experienced accelerated growth in the Internet era thanks in large part to the rise of bureaucratic identity markers and the shift to an information economy (see also Whitson, 2009). The ubiquitous use of computers and their interconnectivity has provided thieves with increased opportunities, and "new channels" (Anderson et al., 2008), to access and misappropriate personal information for the purposes of IDT. The crime has never been easier to commit and public awareness has never been higher, thanks in large part to

high profile incidents of corporations losing control of customers' personal information.

In addition to its high profile, IDT is more often than not "something that affects the ordinary citizen" (Hooley, 2002 cf. Newman & McNally, 2005). Concerns flowing from this lived experience of harm are amplified by the "high-tech" nature of the crime. Where Canadian lawmakers have attempted to quell the growing concern and fit the crime within non-identity specific and traditional criminal provisions such as fraud, forgery, mischief to data, illegal access or imposture (Koops et al., 2009), most of Canada's provisions predate the computer and Internet. Accordingly, policymakers have begun to reevaluate their specific approaches to IDT and seek new answers to the problem.

Correspondingly, much of the debate around IDT is a debate around technological identity. Within a digitalized culture, "data doubles", dense and disembodied entities, circulate within information networks that can be intercepted and compromised (Schwartz, 1999; Whitson & Haggerty, 2008). Traditional social markers of identity, such as relational status or acquaintance, have been systematically replaced with random numerical sequences. This resulting disembodiment has led to increased risks of impersonation and fraud in the e-commerce model. These risks have, consequently, created a number of opportunities for motivated offenders to criminally exploit new information systems (May & Headley, 2004: 45). According to Monahan (2009), any analysis of IDT must understand this transference as a first-order-of-business; however, in order to reach any specific conclusions about the crime and what its impact is on individuals, one must also examine and understand the way IDT is socially and individually problematized by government and the private sector within the policymaking process, as well as the power implications associated with such conceptualizations.

In broad terms, IDT refers to all types of crime in which someone wrongfully obtains and uses another person's identifying information for the purpose of criminal

activity, typically for economic gain (Public Safety Canada, 2008). There are a plethora of definitions of IDT, specific to individual agencies with responsibility for policy development, including, for example, the Royal Canadian Mounted Police, Privacy Commissioner of Canada, Canadian Bankers' Association and the Canadian Chamber of Commerce (see Winterdyk & Thompson, 2008); and as of yet, a consensus has not arisen. Additionally, a number of amendments to the Criminal Code have been proposed, most recently Bill S-4, to define the crime of IDT and deal with the problem more effectively. As such, it is both necessary and sagacious to critically assess the specific ways in which policymakers are articulating and constructing the problem of IDT.

This thesis explores the ways in which two policy institutions, the Consumer Measures Committee (CMC) and Royal Bank of Canada (RBC), define and discuss the problem of IDT and articulate the risk-management techniques required to deal with the defined threat. By examining policies as social artifacts, I identify the claims made by the two institutions and the ways in which they problematize IDT vis-à-vis both old and new risk knowledges. In doing so, I focus on exactly what is being discussed, how the problems are being presented within the policies and what solutions are to be implemented to prevent and respond to the problem. This thesis does not attempt to understand the social process of problematizing IDT, but rather examines policy documents produced by key stakeholders for dissemination to Canadian consumers.

My project is rooted in a social constructionist point-of-view, which seeks to understand how IDT has been constructed as an easily recognizable problem with easily recognizable solutions. I am also interested in exploring the various mechanisms of neoliberal governance contained within the solutions. Given increased technological means to commit the crime, this thesis aims to reveal how the crime is constructed and supported institutionally in relation to individual consumer's online risk concerns and notions of self-governance. Additionally, I attempt to further criminological research into

IDT as a social phenomenon, paying particular attention to its construction as a problem plaguing individual consumers and elucidate the best practices and solutions as determined by powerful institutions who are implicated in constructing the emerging electronic marketplace. Specifically, this thesis seeks to answer the following questions:

- How do key policymakers define the meaning of IDT?
- How do they define the causes of IDT?
- What do they see as the solutions to IDT?
- What are the similarities and differences of the CMC and RBC regarding the construction of IDT?

The paper is organized as follows. Chapter two includes a review of the claims being made in regards to IDT including incident rates and financial costs. I draw from the disciplines of criminology, political science, economics, sociology and legal studies. The chapter begins with the various definitions of the term "identity theft" and then explores the claims in which the disembodiment of digital identity is tied to discourses about the transformative power of the Internet for business, social and criminal practices. I, then, provide an overview of the theoretical understandings of data-doubles, information-networks, power, responsibility and risk, and explore claims that these have allowed IDT to occur with increased frequency.

The remainder of the paper is organized as follows. In chapter three, I outline the methodological approach to the research, including how I selected the sample and the qualitative method employed to identify and analyze the policy discourses presented within the publicly available documents. Chapter three also sets out my theoretical model of analysis, which draws heavily on Best's (2008) social problems and claimsmaking process, and addresses issues with regards to reliability and validity.

Chapters four and five present the original research findings of my qualitative analysis, grouped by theme, while a cross-sectional discussion and conclusion are presented in chapter six and seven. Limitations of the study and possible directions for future projects are also included.

CHAPTER 2

2.1 *Attempts to Define Identity Theft*

Previous attempts to define IDT have been criticized primarily because they are far too simplistic (May & Headley, 2004) and do not classify it as a "stand-alone crime" (Hoofnagle, 2007: 108); the term is often understood to include many different types of crime including check and credit card fraud, medical insurance fraud, theft of automobiles by fraudulent documentation, real estate fraud, and utilities fraud among others (Newman & McNally, 2005; Newman & Clarke, 2003; Pontell, 2009). As such, understanding IDT as a standalone crime has proved difficult in the past and has continued to cause problems in establishing accurate incident rates.

The term "identity theft" itself compounds the problem since it connotes something that typically cannot be stolen; Koops and Leenes (2006) claim that, unlike theft, where the owner loses possession over the stolen good(s), the victim of identity theft still retains his actual identity. Accordingly, the crime has in some instances been understood as identity *takeover* or *misuse*. Because the 'theft' includes vast use of false identifiers and false identifying documents, it has been characterized by some as a narrower subset of identity fraud, entailing the use of a real person's identity, identity theft, and use of a fictitious identity (Main & Robson, 2001, Cabinet Office 2002; CIPPIC, 2007b). Canada's Department of Justice highlights the distinction:

> [identity theft] can refer to the preliminary steps of collecting, possessing, and trafficking in identity information for the purpose of eventual use in crimes... Identity theft in this sense can be contrasted with 'identity fraud', i.e., the subsequent *actual deceptive use* of the identity information of another person in connection with various crimes. Identity theft therefore takes place in advance of and in preparation for identity fraud [emphasis in original] (DOJ, 2007).

Newman and McNally (2005) claim that identity theft and identity fraud, as concepts, appear to be used interchangeably by some institutions (which we will see), reporting agencies, and academics, further complicating matters.

2.2 *Bill S-4 and a New Definition*

Bill S-4: An Act to amend the Criminal Code (identity theft and related misconduct) represents a great leap forward in regards to IDT for Canada. The bill, formulated in April 2009, was passed by both the House of Commons and Senate, and received Royal Assent on 27 October 2009. Created in the wake of Bill C-27's death on the Order Paper when Parliament dissolved on 7 September 2008, the Bill has been praised by Canada's Justice Minister, Rob Nicholson, as it "will better address identity theft and provide police with the tools they need to stop these crimes before they are committed" (DOJ, 2009). The act creates three new "core" Criminal Code offences targeting the early stages of identity theft, all subject to 5-year maximum prison sentences:

1. Obtaining and possessing identity information with the intent to use the information deceptively, dishonestly or fraudulently in the commission of a crime (Clause 10 adding new subsection 402.2(1) to the Code);
2. Trafficking in identity information, an offence that targets those involved in the transmission, making available, distribution, selling or offering for sale, or possession of another person's identity information with knowledge that, or being reckless as to, the possible criminal use of such information (Clause 10 adding new subsection 402.2(2) to the Code);
3. Illegally possessing or trafficking in government documents that contain identity information of another person (Clause 1 adding subsections 56.1(1) to 56.1(4) to the Criminal Code).

Clause 10 also adds a new section to the Criminal Code under the heading "Identity Theft and Identity Fraud", highlighting the important distinction between the two and attempting to reach a newfound understanding of the two terms. Relying heavily upon the distinction made by Justice Canada, the provisions posit that identity theft refers to the preliminary steps (e.g. the collection and possession of another person's identity

information), while identity fraud refers to the subsequent and deceptive use of such information in connection with crimes such as impersonation, fraud or abuse of credit/debit card data.

The definition found in Bill S-4 situates IDT as the precursor to identity fraud and focuses on the preliminary stages of information gathering and the notion of its potentiality for use in later crimes. Focusing solely on the actual commission of a crime using false identifiers, just as Public Safety Canada (2008) tends, precludes the possibility of stockpiled information waiting to be used, illegally, at a later point in time. Where identity fraud is framed as the unlawful use of personally identifying information for illegal or improper purpose, IDT can occur regardless of the information's actual use, noting that the information need not be used illegally in order for "identity theft" to have actually occurred.

While Bill S-4 has justified its use of the term "identity information" from a criminal law perspective, and distanced itself from an invasion-of-privacy perspective (and a subsequent inclusion of "personal information"), the Bill fails to distinguish between what can be classified as personal and identifying information (especially in regards to one's name, date of birth and address which is understood by Bill S-4 as identifying information). The Bill defines identity information as "any information—including biological or physiological information—of a type that is commonly used, alone or in combination with other information, to identify or purport to identify an individual (Clause 10). In so doing, the Bill is "really constrained by the notion of its applying only to information that can identify a person as opposed to information about a person" (Klineberg, 2009) and claims that a clear delineation exists between the criminal law sphere and the privacy sphere with respect to IDT.

2.3 *Incidence Rates*

Studies have claimed that, in addition to the conceptual problems associated with IDT, procedural issues have also led to highly skeptical and unreliable official numbers on IDT. Not all cases of IDT ever come to the attention of victims, and when they do, most victims choose not to report the crime with estimates of roughly 75 percent of incidents never coming to the attention of police (Synovate, 2003). Furnell (2007) claims that even when individuals choose to report, they most often report the incident solely to banks and credit institutions. Foley (2003) has offered particular reasons for this, suggesting that the realization that a crime has occurred usually stems from a bank statement, denied credit application or proactive business practice, conceptualizing IDT as a de facto financial concern. Any changes in occurrence rates may therefore, as a result, represent merely a change in the rate of reporting the incident.

Despite such setbacks, there nonetheless exists a great deal of consensus on IDT's prevalence. Certainly, it is a crime that is garnering considerably more attention in the news headlines, having claimed the title of the fastest growing crime today (McWaters & Ford, 2007: 19). A search of Canadian Newsstand using the ProQuest search engine for the term *identity theft* found an marked increase in articles with at least some coverage of the issue (1994 saw 0 articles, 2000 saw 71 articles, 2004 saw 880 and 2006 saw 1,203), while a similar search of Canadian Business and Current Affairs saw a similar trend from 2002 to 2006 (Winterdyk & Thompson, 2008: 155); the media is making an increased number of claims with respect to IDT. A search of articles using the Lexis-Nexis U.S. Newspapers database revealed an even more substantial increase with 30 articles in 1995, almost 2,000 in 2000 and more than 12,000 in 2005 (Anderson et al., 2008: 171). In light of such increases, the crime is understood to be a hot-topic of discussion, having secured the attention of the media and public—an important step in reaching policymakers.

Surveys produced by the Federal Trade Commission (2003, 2006) and Javelin Strategy and Research (2007) also claim to offer some evidence of the rates of IDT. Of the FTC's randomly selected individuals, 3.7 percent of respondents reported being a victim within the previous year (FTC, 2006), suggesting that in the U.S. alone, some 8.3 million adults actually discovered and reported misuse of their personal information during 2005. Javelin (2007) found that incident rates ranging from 4.25 per cent in 2004 to 3.74 percent in 2006, while other data from the U.S. claims that as many as 27 million Americans fell victim to identity theft from 1999-2003, with more than 10 million cases in 2003 alone (Gerard et al., 2004).

While IDT is most often portrayed as a crime directly targeting consumers, studies suggest that rates can be largely accredited to data breaches, with up to 70 percent of cases attributable to data mismanagement at the corporate level (Haggerty, 2007; Whitson, 2009). Of particular interest, a 2009 Data Breach Investigations Report from Verizon Business revealed that criminals secured 285 million personally identifying records in 2008, more than Verizon Business had found to be stolen in the previous four years combined (Larkin, 2009). Moreover, the Identity Theft Resource Center in the U.S. found that the total number of reported data breaches, ranging from lost laptops to massive data thefts, leapt 47 percent in 2008 from 446 breaches in 2007 to 656 in 2008 (*ibid*). In similar fashion, Schreft (2007) has detailed increases in the number of compromised company records from 2001 to 2007; this supports the claim that IDT typically occurs indirectly, through systemic exploitation rather than individual consumer targeting.

The Royal Bank of Canada reported that in Canada alone, there were in excess of 2 billion fraudulent credit card and debit card transactions in 2005 (Moneris Solutions, 2006)—but RBC's figures are merely the result of actual transactions that manifest. Additional claims have been made by Phonebusters, Canada's Anti-Fraud Call Center,

which is jointly managed by the Ontario Provincial Police (OPP), Royal Canadian Mounted Police (RCMP) and the Competition Bureau of Canada; Phonebusters (2009) claimed that total Canadian victims of IDT increased from 10 328 in 2007 to 11 463 in 2008, but experienced a slight drop off to 11 109 incidents for 2009; however, their figures are entirely complaint-based. The information varies broadly, and figures on IDT in Canada must, for our purposes, be treated as claims and not facts.

2.4 *Costs of IDT*

There is a general consensus that the monetary value of losses associated with IDT has continued to increase over recent years (Winterdyk and Thompson, 2008). Despite a recent dip in the number of complainants, Phonebusters (2009) claimed that the total dollars lost in conjunction with complaints increased for 2008-09 leading them to purport that identity thieves are becoming more successful in securing larger scores; the losses have increased steadily from $6,467,387.75 in 2007, to $9,625,837.05 in 2008, and $10,882,279.04 in 2009 according to their reports.

May and Headley (2004) break down costs to businesses to include direct losses (such as false accounts and fraudulent transactions), loss-avoidance costs (such as hotlines, taskforces, education), and indirect costs (loss of consumer confidence, less frequent bank use). The costs of IDT to businesses vary greatly according to Anderson et al. (2008) with some claiming losses in excess of $100 billion annually and others claiming a figure of approximately $200-$250 billion (Bocij, 2006: 93). Synovate (2003) found that some polls of costs to victims and businesses ranged from $47 billion per year to approximately $280 billion per year illustrating the disparity. Claims are, therefore, contradictory and vague; as Hoofnagle (2007) notes, the sheer number of claims being made about IDT make the scope and severity of IDT largely a known-unknown.

Costs to the government are similarly treated as unknown and, to a certain extent, unknowable. Any determinations that are made are done so using best-guess positions. The cross-jurisdictional and transnational nature of IDT serves only to undervalue the costs of investigation, prosecution (May & Headley, 2004), cooperation and coordination among federal, state, and local law enforcement agencies (GAO, 2002); monies spent by the government on working groups, public education, departmental resources and salaries are, therefore, presented as "incalculable."

While businesses and governments are victims of IDT too, it is the individual who represents the most visible victim since it is their identity that is effectively "stolen." Javelin (2007) claims that through the misuse of stolen personally identifying information, thieves obtained $5,720 directly from the average victim through fraudulent transactions. While victims are not held responsible for fraudulent charges once the banks are satisfied their customers were not accessories to fraud, they do bear the responsibility for clearing their names and restoring their credit records to their previous levels—which can range from 30 hours (Synovate, 2003) and $500 to upwards of 23 months according to expert think-tanks (CALPIRG, 2000) depending on the specific type of crime committed. In addition to the direct financial costs, Foley (2003) claims that there is often an overwhelming violation of personal space and invasion of privacy reported by victims as well as a sense of dread when they are asked to disclose additional information in subsequent situations, marking the healing process of IDT as long, tedious and exhausting for victims.

2.5 *Re-Thinking the Crime*

Recent studies have claimed that 70 percent of US citizens rate the likelihood of their being a victim of a cybercrime higher than the likelihood of their being a victim of a

physical crime[1] ("More Americans"), and that the average Canadian citizen is also more likely to be victim to a cybercrime than a street or domestic crime[2] (Deloitte & Touche, LLP, 2008). In those surveys, respondents have voiced a personal concern in being victim to IDT as a result of direct targeting (Mayer, 2006; Deloitte, 2008), while others have highlighted personal misgivings in using credit cards online (Statistics Canada, 2006; Horrigan, 2008). According to Harris (2004), such fear arises out of a concerted and generalized fear in e-commerce transactions (despite its high prevalence), with users fearing that their personal information could easily be stolen. This is consistent with the position of the OECD (2008) that information today is more transparent and transferable than ever before. Many of the surveys focus generally on privacy concerns vis-à-vis information sharing, e-commerce, and online banking, finding generalized fear among respondents. However, Harper and Singleton (2001) warn that such surveys do not offer precisely operationalized concepts, which often leads to manipulability given the almost universal use of questions. Because of this, a clear delineation between fact and fiction cannot be made. There are a plethora of discourses being mobilized, and these discourses (and their claims) are preventing researchers from establishing accurate facts about the phenomenon.

2.6 *What's Different Now?*

While the idea of IDT is not new, having existed in various forms for centuries (Benson, 2009), a number of agencies claim that it has changed markedly since the early 1990s. The question then becomes: why the *sudden* change in the 1990s?

---

[1] Opinion Research Corporation conducted this survey on behalf of IBM. A total of 679 telephone interviews were conducted with adults (337 males and 342 females) aged 18 and over, living in private continental-US households. Completed interviews were weighted by four variables: age, sex, geographic region and race to ensure a reliable and representative sample. Questionnaire consisted of 10 closed-ended questions, and was fielded at the 95% CI, margin of error of +/- 4 per cent.

[2] The survey, conducted by Deloitte LLP, consisted of three components: an Ipsos Reid market research survey of 587 Canadians, interviews with 63 key contacts throughout law enforcement, prosecutions, government, academia and industry, as well as an analysis of open source survey data.

For some, the answer lies in the surrounding landscape; Pontell (2009) argues that technological advances in information technology/storage/transmission coupled with structural changes in the financial services industry increased the relative value of identities and the ease with which they could be appropriated, used and stolen. Meanwhile, Newman and McNally (2005) agree, claiming that the very nature of the crime makes it considerably more appealing in light of marked changes in technology, communication, and commerce. According to them, there are three main attractions for identity thieves in particular: anticipated rewards, the advantage of intrinsic concealment, and comparatively mild sentences to other crimes (*ibid*: 46; see also Craats, 2005: 39). Additionally, Newman and Clarke (2003) claim that identity is now a "hot product" CRAVED by thieves: Concealable, Removable, Available, Valuable, Enjoyable and, lastly, Disposable. They also argue that the system in which identity products reside offers the following benefits, making IDT a logical choice: Stealth, Challenge, Anonymity, Reconnaissance, Escape and Multiplicity (SCAREM) (Newman & Clarke, 2003). As such, it is claimed that the crime itself, the systems it exploits and the very characteristics of an identity in today's market economy have made IDT a highly attractive and lucrative criminal venture today for motivated individuals, contributing heavily to its growth in recent years.

These claims have led to increased responses in policing and prevention (see Chua, 2003; Henderson, 2005; Mayer, 2005; Saffran, 2005). Websites that offer the transaction option now also include helpful tips and recommendations for customers to follow to guard against misuse of their information, and a range of consumer-protection agencies (including Industry Canada) have rallied for a more-secure consumer experience. Law-enforcement responses typically follow situational crime prevention methods. Enterprises such as CPTED, crime prevention through environmental design, and RAT, routine activities theory (South, 1987; Felson, 1998; Hughes, 1998), have

aimed to target IDT through loss prevention, target hardening and enhanced guardianship. And while never proven to be true, the Internet, according to police and banks, has presented a dramatic challenge to authorities as it appears to harbor numerous motivated and anonymous offenders, lacks effective guardians (who partner effectively—see Gill et al., 2006 and Van der Meulen, 2006 for support), and presents large numbers of suitable, hapless and vulnerable targets.

2.7 *Accessibility of Knowledge*

Identifying the extent of IDT is deemed problematic because it relies "entirely on self reporting on the part of victims" (May & Headley, 2004: 43) who oftentimes do not even realize they have fallen victim to IDT until an application for employment, loan or mortgage comes back as denied (Shoudt, 2002). Despite the concerted efforts to quantify IDT and estimating total costs (Javelin, 2007; Synovate, 2003 among others) by way of self-report and victimization surveys, existing studies on prevalence suffer from a "fundamental lack of data access" (Hoofnagle, 2007: 104) to information possessed by financial institutions, those with the most information on IDT (*ibid*), and those who are able to tell consumers that their cards have been compromised. As such, the fact cannot be separated from fiction within the claims being made about IDT. And because of this, we cannot understand IDT within the world of social facts and must, therefore, treat it as a social construction.

Financial institutions are not required to report their total losses or cases of data breaches to the government, public, industry counterparts and other key stakeholders (Lacey & Cuganesan, 2004) except in cases where privacy laws apply. In January 2007, TJX Cos., the U.S. parent firm of Canadian retailers HomeSense and Winners reported one of the biggest cases of data breach only because the parent firm was subject to U.S. privacy laws. According to Clarke (2001) and Hoofnagle (2007), businesses are reluctant to report information misuse, IDT or data breaches because of embarrassment or

corporate reputation. As a safeguard, businesses often treat crimes such as shoplifting, credit card fraud or data loss as a cost of doing business, factoring such crimes into inventory loss or shrinkage (Newman & McNally, 2005: 47). Police, too, are prone to such lumping practices; with no comparable training, the offence of IDT is often misclassified or lumped together with broader offences such as fraud for purposes of data management and assimilation (CIPPIC, 2007b: 17).

Schneier (2004) argues that businesses should be required to proactively disclose IDT information since they too are victims and are better able than consumers to become aware of suspicious activities and IDT (Lacey & Cuganesan, 2004). However, in doing so, institutions may become less accepting of victim's claims in an effort to make their IDT rates appear lower, making victims accountable for the fraudulent charges (Solove, 2007). Better information on IDT as a whole may cost businesses in the long run, and may be a primary reason why they remain hesitant to report all known incidences. Until then, accurately understanding how many have fallen victim to IDT and the associated costs remains impracticable.

2.8 *The Transforming Power of the Internet*

While many of the identified aspects of information economy are not new—e.g. identifying information, transaction systems—there have been a series of recent innovations that represent drastic discontinuities with earlier times, the Internet and online banking being but two examples.

As a digital medium, the Internet "brings about a form of social being and a set of social actions that is different from other forms of being and action" (Dant, 2004: 70). It represents a blending of cyber space and real-world space (Steeves & Wing, 2006), a social conduit, portal and, ultimately, a source of power to each individual user (Heuston & Block, 2009). The Internet, from these perspectives as well as others, holds great potential in looking at (technologically) social, political and consumer relations from an

empowering, neoliberal perspective. Examining how individuals are implicated online within neoliberal forms of governance, as this study attempts, should lead to enhanced consumer education about why things are the way they are, why website terms are constructed the way they are, what ramifications they can have for individual users, and how consumers may naturally, and inadvertently, contribute to IDT online.

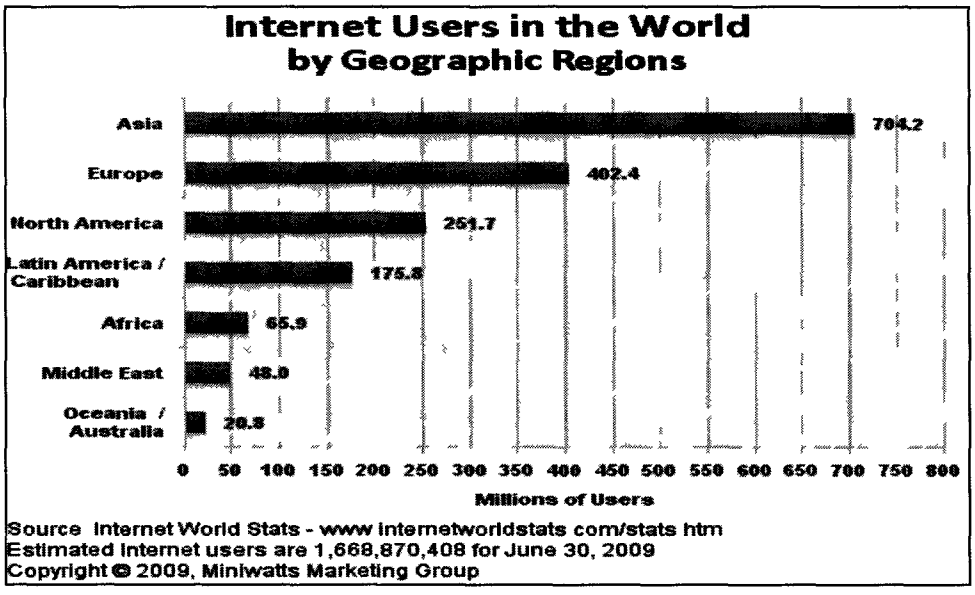
The growth of the Internet has risen dramatically in the past decade to the point of becoming an addiction (Young, 1998) and more of a necessity to daily living (D'Amico, 1998). The Internet has continued to transform notions of time and space—including the increased ability to disseminate information through personal, social and financial accounts, email and readily-accessible newsfeeds and websites just as telegraphs and telephones did previously. As Sikka (2006) argues, the Internet has created similar possibilities for emancipatory education and repositioning of social subjects by eliminating additional territorial boundaries, helping to expand and rejuvenate the public sphere (Habermas, 1989; Hayden, 2002) and expose that which was previously confined to the private realm—making the private, public and making IDT more of a concern and reality. The newfound sense of technological life resonates in the writings of Lash (2001) and Marx (1995), who argue that we now make sense of the world through these technological systems and have equated progress with new technology, embracing these systems as self-evident solutions to complex social problems. Technological breakthroughs may been seen as revolutionary in their own right, but Haggerty (2004a: 224) maintains that they represent more of a change in degree than a change in kind, more of a "convergence and intensification of social tendencies" that have rooted themselves in history, and have, therefore, allowed individuals, as well as criminals in cases of IDT, to better meet their needs.

The effect of the Internet as a communication medium on individuals relies mainly on that person's reasons and goals for using that medium (McKenna & Bargh,

2000); because the reasons people use the Internet vary across the board (i.e. entertainment, social networking, business, reading news from around the world, etc.), there will, undoubtedly, be a plethora of outcomes which can be said to be neither entirely good nor entirely bad (*ibid*) nor even foreseeable. It is conceivable (and perhaps most probable) then to understand the Internet as a medium towards goal-attainment, as a tool of everyday life to help make users' lives that much less cumbersome and that much more convenient.

Despite the convenience, there are concerns that the Internet represents a "Pandora's box of issues and challenges" (Pennathur, 2001: 2107), contributing heavily to deindividuation, a process which occurs when individuals feel extricated from full responsibility for their actions because they no longer possess an acute awareness of their self, others, or their social environment that provides the context for the behavior (Hiltz et al. 1989; Diener, 1980; Postmes et al., 1998); this results in: a weakened ability to self-regulate behavior, a reduced ability to engage in long-term, rational planning, and a tendency to react to immediate cues emotionally (Zimbardo, 1969), decreasing the influence of internal standards (Johnson & Downing, 1979) and leading to risky behaviors. Deindividuation concerns stem from the development of the "reduced social cues" model formed by Kiesler (1986), which sees the Internet as incomplete, lacking important and necessary social information. Such processes play an important part, as will be seen, in guarding against IDT according to the institutions studied below.

The Internet's reach is extensive with over 1.66 billion users worldwide and growing. Statistics from 2007 found that over 68 percent of Canadians use the Internet daily (Statistics Canada, 2008a) with 78.6 percent of those aged 34 and under using it daily. Moreover, with broadband technology exceeding 90 percent of Internet users in many western markets (Ovum, 2006), the world today is becoming increasingly wired and technologically-savvy.



(Figure 1)

Because the Internet is a digital medium, the individual is usually required by law to authenticate their true identity, that which distinguishes them from everyone else. This can happen two ways according to Clarke (1994, cf. Kahn & Roberds, 2005): either through knowledge or token. In knowledge-based models, the individual is required to provide information about him/herself that only they would be expected to know (e.g. mother's maiden name, place of birth, birth date). On the other hand, one may be required to provide documentary evidence of a previous encounter/identity (providing a birth certificate or passport for instance)—a token, of sorts. Consumers must, therefore, resort to proving their identity using such tokens in order to interact on a continued basis (Lacey & Cuganesan, 2004) even if the proof required is minimal; often, information such as full name, DOB, and a valid email address is all that is required to create an authenticated "online identity." Hotmail, the world's largest free email provider, requires but one's first and last names, zipcode, state and country, as well as gender and birth year to create an email address—all of which can easily be falsified. Once created, an online identity is born.

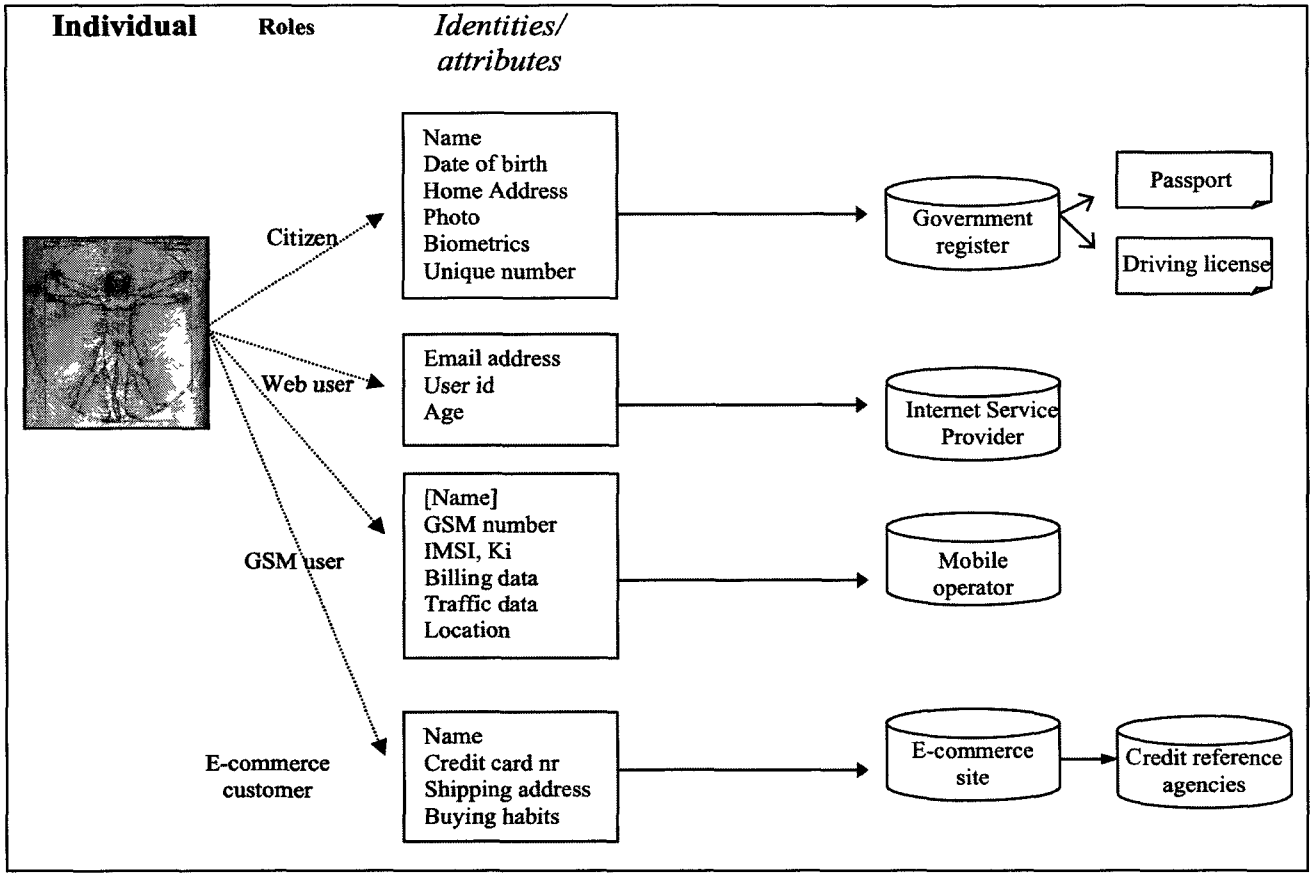
2.9 Data Assemblages

Use of such identifiers is based on the idea of an information economy (Whitson,

2009), a system of individual identity markers and data-doubles; the data-doubles, or identity traces, emanate from the body which is "broken down into a series of discrete signifying flows" (Haggerty & Ericson, 2000: 612); the result of which is the "multiplication of the individual, the constitution of an additional self" (Poster, 1990: 97), and the dissolution of purely embodied personhood (Capeller, 2001) through the process of constant "gathering, individualizing, differentiating and generalizing enormous amounts of personal and conjectural information" (Los, 2006: 91). In this sense, these types of information are reconstituted as power (Samarajiva and Shields, 1992), but requiring continual management in order to stabilize any effect (Latour, 1991) and prevent the misuse of personal, individualized information for criminal purposes such as IDT. As Caeton (2007) notes, "as the phrase *identity theft* indicates, what is at stake is not merely property but rather the intimate information that qualifies an individual for recognition by the institutional infrastructure that undergirds the public and private realms of contemporary society" (pg. 12). It is these pieces of information that are reducing individuals to easily stored, synthesized and monitored collections of data and of so high value to identity thieves today.

Figure 2 represents an excellent model of identity authentication processes and "interface surveillance" (Lyon, 2006), being able to cover a great deal of the information-interrelationships that exist today. What is important in these respects is to highlight the importance placed on each of the identity attributes in giving the physical person an actual identity and air of truth so to speak. The image uses Rose's (1996a) concept of the cybernetic organism, a "nonunified [sic] hybrid assembled of body parts and mechanical artifacts, myths, dreams and fragments of knowledge" (pg. 5), as the basis for understanding the various roles and attributes of individuals of today. Within the model, the individual comes to understand him/herself through various mental processes (knowing, speaking, enacting and judging themselves according to societal norms)

associated with each of the identities they inhabit, and institutions come to understand each individual in agency-specific terms whether as an upstanding citizen, valued customer, heavy Internet user and so forth.



(Figure 2 – taken from Mitchison et al. 2004: 11)

These processes recount many of the principles of panopticism—including surveillance, control, governance and power—developed by Jeremy Bentham and detailed in the works of Foucault (1979) and Deleuze (1997). Foucault (1979) noted the rise of panopticism and its effect in establishing what he called the "disciplinary society" in institutions such as factories, schools and prisons. He claimed that the major effect of the panopticon was to

> induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power. So to arrange things that the surveillance is permanent in its effects, even if it is discontinuous in its action; that the perfection of power should tend to render its actual

> exercise unnecessary ... [so that the inmate] becomes the principle of his own subjection (*ibid*: 201-203).

Yet, long before Bentham's panopticon rendered the individual as manageable and transparent, Petty's "London Wall" (from his notes in the 1670s and 1680s c.f. Rigakos and Hadden, 2001) spoke of the economic necessity for knowing a given population; the Wall was a means for "concentrating commerce by channeling it through planned choke-points, where all movement could be made visible and all trade accountable" (Rigakos & Hadden, 2001: 69-70). Such thought conceived of the inhabitants—the objects of governance—in terms of their own individuality, including unique signatures, birth certificates, or other identifiers (Jones, 2000) so that they may be governed effectively as an expression of actuarial management and need to control dangers (Foucault, 1979; Rigakos & Hadden, 2001; Norris & McCahill, 2006). The Wall and panopticon reflect the specific brand of politics closely associated with conservative brands of neoliberalism (O'Malley, 2008: 453), the actuarial knowledge of populations as well as their accompany risk-groupings (Garland, 1997). It is this line of reason that ties in the discourses associated with actuarial management, panopticism, neoliberalism and risk quite nicely for purposes of understanding how identities are produced and managed in an information economy.

In the digital age, these management principles still apply, but instead of being understood as unique entities, individuals are now understood as dividuals, masses and samples of data (Deleuze, 1990). So instead of individual signatures, we have PIN numbers and passwords that grant access to our personal information and financial resources. With the commodification of digital information, especially for the purposes of online banking, Hayles (1999: 78) maintains that the "crucial issue with information is thus not possession but access."

2.10 New Practices

Internet banking is defined as "the ability of banks to use the Internet as an additional delivery channel for banking service and transactions. By doing so, they can reach their customers directly with no intermediaries" (Ciciretti et al., 2009) and grant clients the increased opportunity to access their accounts and self-manage. Pennathur (2001) claims that banks have realized the value of introducing new technologies for old ways of business, complementing the traditional bricks and mortar presence with both 'clicks and bricks.' Researchers have claimed that the move was instituted in order to increase relative market share (Hannan & McDowell, 1990; Bouckaert & Degryse, 1995; Degryse, 1996), reduce costs (Daniel et al., 1973; Hunter & Timme, 1986; Karjaluoto et al. 2003), bolster efficiency (Wheelock and Wilson, 1999), and allow greater control of resources to individual users (Stana, 2002). Coleman and Porter (1996) contend that the processes of globalization, fostered by the neoliberal financial order, have led banks to rethink their traditional approaches and move towards fully-integrated and online services in order to remain globally competitive and maximize efficiency. Having always been receptive to international financial flows, it is not surprising that Canadian banks, such as the RBC, have fostered and followed such a trend (*ibid*) and granted individual clients this power.

In making the move towards Internet banking, banks are forced to weigh the importance of security measures against user-friendliness (Mitchison et al., 2004); as more information and more token-authentications are required to interact online, a website often becomes less user-friendly and hampers widespread acceptance in the process (*ibid*). Such a tradeoff is a constant concern for banks in promoting ease of use with their offered services. Bauer and Hein (2006) claim that utility-maximization and risk aversion are the main determinants in deciding if and when consumers adopt and support new technologies such as Internet banking; accordingly, banks want to ensure

that their offerings are beneficial yet secure at the same time in order to overcome any initial hesitation in using new services.

Public confidence in the banks and businesses is established through trusted transactions involving personally identifying information (PII) between consumers and businesses as part of normal business, market research, advertising, giveaways, warranties and so forth. Marshall and Tompsett (2005) claim that by necessarily and voluntarily sharing such information a degree (and chain) of trust is formed between the consumer and bank—a chain that is recognized explicitly within various legislative reforms (for review of Canadian legislation see CIPPIC 2007a). In Canada, PIPEDA, the *Personal Information Protection and Electronic Documents Act* formed in the late 1990s, recognizes this chain of trust by way of balancing the privacy rights of the individual with the needs of organizations for PII to more effectively serve customers.

While most people believe that technological systems are synonymous with progress (Winner, 1977, 1986), accepting such a belief tends to neglect the ways in which those systems simultaneously increase vulnerability and information abuses (Haggerty, 2004b) by identity thieves, government agents, employee insiders or others. Despite the legal onuses on private industries to ensure system integrity, Ferguson (2000) has found that they are not always committed to detail-oriented approaches required to ensure security and guard against IDT. The studies of Perrow (1984) and Schreft (2007) have attempted to explain such failures in the context of information technology; according to them, information technology compounds system complexity, making organizations more difficult to manage while simultaneously increasing the likelihood of system failure or data breaches. Monahan (2009) concurs but is quick to add that previously relaxed regulations for data protection allowed industries to stockpile and trade personal data, thereby facilitating capital accumulation and increasing data vulnerability at the same time. In light of such findings, Whitson (2009: 45) has

suggested that corporations should not simply ask themselves "should we collect this data just because we can?" but, rather, should calculate the benefits of collecting and storing it versus the risk of such information falling into the wrong hands since it has been claimed that most cases of IDT result from information lost through the careless data management practices of major institutions (Haggerty, 2006) with estimates up to 70 percent (see Collins & Hoffman, 2004: 6; Jewkes, 2003). It is these type concerns—information practices and economic trends—that are to be considered if one is to understand policymakers' conceptualizations of IDT.

2.11 Online Self-Efficacy

Pennathur (2001: 2107) claims that Internet banking is something that "web-savvy customers demand." Responding to the neoliberal forms of governance, individuals have begun to seek out commercial solutions to their personal matters (O'Malley, 1992), and organizations have been quick to formulate a marketing campaign designed to capitalize on this need (Haggerty, 2004; Monahan, 2009). But by agreeing to an organization's terms of use and policies, individuals have entrusted themselves with ever-increasing power to police their own net-safety by building concepts of self-efficacy, meaning "the belief in one's own ability to carry out an action in pursuit of a valued goal, such as online safety" (Larose et al. 2008: 72). Such belief has a direct impact on safe behavior, but has to also interact with personal risk perceptions (*ibid*) in order to affect change and direct responsible behavior (Witte, 1992). Bombarding the individual with fear messages and online safety may bring about change, but Larose et al. (2008) claim that it is only when the individual becomes deeply involved in the subject of online safety, that they are likely to weigh all the pros and cons of arguments made for and against online safety practices. Therefore, in order to guard effectively against IDT, the crime must be characterized and understood as a cause for personal concern. They claim:

> When involvement of our ability to process information is low, individuals are likely to take mental shortcuts (heuristics), such as relying on the credibility of a Web site rather than reading its privacy policy... The fear shuts down rational thinking about the threat to the point that users may deny the important of the threat and choose unsafe actions (*ibid*: 74).

The average user can be induced to take a more active and responsible role in maintaining online safety as evidenced in a recent U.S. survey, which found that more than 53 percent of Americans, from a representative sample, held themselves most responsible for protecting themselves from cybercrime ("More Americans", 2006). There is little doubt that both organizations and governments have tried to induce such behaviors here in Canada, as well, by highlighting the importance of protecting one's self and one's family online (see the Federal Trade Commission; SafeCanada.ca; Canada's Office of Consumer Affairs; Privacy Commissioner of Canada, Phonebusters).

2.12 *Old Goals, New Ways*

According to Solove (2004), the trends showcased in online banking and information storage have led criminals to exploit the online systems for personal gain and IDT purposes. After all, online business is for all intents and purposes big business; a recent survey (Horrigan, 2008) found that 66 percent of Internet-connected consumers purchased a product online, up from 46% in 2000, meaning that more and more people are conducting business online, volunteering their personal/financial information, and placing the accompanying trust in businesses and their information practices.

According to Pease (2005), the emerging technologies and data practices allow motivated individuals to commit crimes previously beyond their means creating an empowered small-agent, and this new electronic world is understood to make parting a "fool and his money... quicker and easier" (cf. Pease, 2005: 22). Because the Internet has challenged "many of the principle upon which our conventional understandings of crime and policing are based" (Wall, 2001: 6), it is the individual consumer who has been

asked to increase their own policing efforts, paying particular attention to the risks and acting in their overall best interests. The social constructionist agenda, as employed within this study, aims to elucidate many of these foundational constructs, explain them vis-à-vis the claims being made, the evidence purported and the accompanying solutions—including the reorganization of social life and normalization of neoliberal mechanisms of governance as detailed by Monahan (2009).

2.13 *IDT and Governmentality*

Businesses and agencies are understood to enjoy privileged access to information for a number of reasons including larger social and political trends in governance. Where knowledge of a population was once relegated to the government, businesses today have privileged knowledge of their customer bases (and IDT risks, for that matter). According to Foucault (1991a), government, traditionally understood as the institution governing citizens of a nation, has evolved to include all those more or less rationalized programs, strategies and tactics that concern themselves with the "conduct of conduct" and for acting upon the actions of others in order to achieve certain ends (see also Rose, 1996a; Miller & Rose, 1990; Miller & Rose, 1992). Foucault's (1991a) theory of governmentality claims that the movement from a pre-modern sovereign state to a modern governmentalized state was "tied up with the discovery and demarcation of new social entities (the population, the economy) and the development of new social sciences that produce a knowledge of them" (Garland, 1997: 178). Accordingly, individuals were (and still are) willing to do their bit in maintaining such systems that define and delimit them as subjects or consumers, and play their parts in a market game whose intelligibility and limits they take for granted (Rajchman, 1991; Gordon, 1991). Such governance has always, according to Rose (1996a), been linked to a way free individuals are enjoined to govern themselves as subjects of liberty and responsibility led by an invisible hand to promote an end which was no part of the original intention (Smith,

2000). If successful, a liberal state such as this could, and should, maximize individual happiness by promoting individual development, diversity, liberty, and freedom (Mill, 1859, 2006), yet at the same time govern that population in those pursuits. This shift has, according to Coleman and Porter (1996), created a new globally-competitive and efficiency-maximizing market under which individuals now find themselves, known as the neoliberal world order. This study is grounded in a governmentality perspective and accordingly examines how the problem of and solutions to IDT have been discursively constructed by CMC and RBC.

Despite the transformative tones, McMullan (1998) claims that there has been far greater continuity between early modes of governance and modern liberalism or neoliberalism than is often recognized. In pastoral power relations and the welfare state, after all, individuals had always been expected to govern themselves and their dependents (see O'Malley, 2008; Foucault, 1979; Rigakos & Hadden, 2001) just as they are within the neoliberal model, doing all they can to avoid harm and maximize utility; while these characteristics may have existed in actual fact long before neoliberals took notice (with its origins dating back to Adam Smith and his classical liberal model in *Wealth of Nations*), it is the neoliberals' extended focus on the transformation of governance which allows for deeper analysis of IDT, as an unexpected consequence of the political and economic movements, for purposes of this study.

Neoliberalism is a set of economic policies that has received increased favor and support over the past 30 years or so. Highly associated with Reagonomics and Margaret Thatcher, neoliberalism has been the dominant global political economic trend adopted by political parties of the center as well as the traditional right and left wings (Chomsky, 2003). Where the welfare state concerns itself with the well-being of all citizens, with economic safety-nets in place to level the playing field, a neoliberal system claims a shift towards making the market fundamental in governing all aspects of life including the

economic, social, political, and even religious spheres as necessary (Harvey, 2005).

Neoliberalism is specifically understood as a set of policies, systems and beliefs that enforce and justify the following: state withdrawal from the provision of social welfare (Bourdieu, 1998; Katz, 2006; Martinez & Garcia, 1997); privatization of public services, public spaces and public resources (Graham & Marvin, 2001; Giroux, 2004; Monahan, 2005); increasingly disciplinary control and surveillance of risky populations (Garland, 2001; Wacquant, 2001; Haggerty, 2004a; O'Malley, 2004; Simon, 2006; Hannah-Moffat, 2000); and, most important to this study, the redefining of citizen rights as consumer choices and the citizen into a *homo economicus* (economic man who is manipulable) in order to meet basic needs or solve problems (for further reading see Rose, 1999; Comaroff & Comaroff, 2000; Duggan, 2003; Garland, 2003; Brown, 2006; Fisher, 2007).

According to Sikka (2006), this set of policies, systems and beliefs was set in place to solve an eroding sense of independency and individual responsibility created by the Keynesian welfare state. In doing so, traditional functions of government—even those relating to policing, security, incarceration, health and education—were handed to institutions and individual citizens. The institutions were primarily concerned with maximizing profits and appeasing the free market, while individual citizens were asked to act in a responsible fashion as self-interested and self-governed agents to ensure their own physical, emotional and economic well-being, basing their decisions on rational, responsible, prudent and free choice (Rose, 1993; Hannah-Moffat, 2000). In doing so, the individual became what Foucault (1991a) termed the target of government. That is to say, Foucault identified the process of individualization which is intelligible less in terms of new social relations than by reference to its positive promotion by a professionalizing political technique: a government of individuals and their marginal-utility vis-à-vis the objective of strengthening the state by maximizing each person's appropriate and

particular contributions to the unit (state) as a whole, thereby making state and individual contractual partners (Burchell, 1991; Hobbes, 1991). Understanding one's life as an individual enterprise, part of the continuous business of living to make adequate provision of one's own human capital, the individual was entrusted with "caring for the self", the governmental correction to collective greed (Foucault, 1988). As Burchell (1991) continues to note, individuals

> must pursue their particular interests as far as possible since this will increase the interests of all other individuals. The pursuit of private interests by each individual operates according to a mechanics which spontaneously multiplies the possible objects and means of satisfying interests, and which results in a spontaneous co-ordination of the will of each with the wills of all other economic subjects (p. 132-133).

Instilled with this power, the individual has seemingly been granted an array of options from which to choose, according to Garland (2003); Foucault (1982) maintains that such power, exercisable only through free individuals, has resulted in a "field of possibilities in which several kinds of conduct, several ways of reacting and modes of behavior are available" (342); but while freedom of the individual may be a key characteristic of a neoliberal agenda, the newfound freedom is not necessarily free in the traditional sense of the word. Evaluation and scrutiny of such choices invariably follow, resulting in a further suppression of freedoms in line with authoritative norms and marking the state as both "individualizing and totalitarian." To rule effectively and democratically, according to Rose (1996a), is to rule individuals through their freedoms and choices rather than despite them—to align their motivations and interrelations, as potential sites of resistance, with political objectives and turn them into "allies of rule." He continues to note the

> forms of freedom we inhabit today are intrinsically bound to a regime of subjectification in which subjects are not merely 'free to choose' but obliged to be free, to understand and enact their lives in terms of choice under

> conditions that systematically limit their capacities of so many to shape their own destiny (1996a: 17).

Foucault's (1979) analysis of early liberalism indicates the ways in which the political objectification of individuals as members of a larger flock, as rational interest-motivated economic beings, and so forth, have rendered us governable and amenable to instruction, discipline, and directed guidance in the pursuit of optimal conditions (Burchell, 1991) without our conscious knowledge. Moreover, Rose (1996a) maintains that in having one's conduct shaped by programs, policies and proposals, one also becomes "more intelligent, wise, happy, virtuous, healthy, productive, docile, enterprising, fulfilled, self-esteeming, empowered" (pg. 12)—all attainable within the governmental model. In this sense, shaping the conduct of individuals and having them buy into the process becomes important to the health and well-being of individuals, which is understood "as having vital consequences for national wealth, health, and tranquility" (*ibid*: 100). This shaping of conduct cannot happen without knowledge, which plays a key role in the contemporary conduct of conduct; specifically, any legitimate attempt to act upon the conduct of individuals must "embody some way of understanding, classifying, calculating" (*ibid*: 12) a problem and the accompanying solutions.

In order to manage one's well-being, one must be conscious and aware of the various risks that may arise. Where risks in the past may have been determined, and subsequently, managed by the state, decisions geared towards the management of risk are becoming increasingly dependent upon the production of the individual's own risk knowledge according to O'Malley (1996) and Ekberg (2007). The empowered individual agent (Foucault, 1980) who is ready and able to guard against risk must, therefore, seek truth—e.g. knowing what to guard against, what solutions work and which do not. But these truths do not, necessarily, self-actuate; often, the individual comes to this

knowledge through the encoded norms and expectations of society (Rigakos & Hadden, 2001), made available to all citizens through their own pursuits as well as the vast dissemination of discourses, practices, and techniques in everyday society by authorities (e.g. giving your name and passwords to online banking sites considered unsafe, installing deadbolts on front entrance door considered safe). Authority, in the neoliberal model, becomes not so much a matter of ordering, controlling and commanding the obedience and loyalty of individuals, but of "improving the capacity for individuals to exercise authority over themselves... to understand their own actions and to regulate their own conduct" (Rose, 1996a: 63-4). As such, each individual is invested with their own degrees of power, authority, and autonomy so as to make the right choices in the market economy. No longer a passive recipient of instructions, individuals are actively engaged in efforts to achieve economic, political and social harmony (*ibid*: 136). By being granted these tools, one must also seek the various systems of (or institutions in) power, the mechanisms of governance which produce and sustain the elements of truth according to Foucault (1980), and the use of symbolic power which is the control of what counts as legitimate representations of reality according to Bourdieu (1998). Monahan (2009) maintains that the crime of IDT actively structures these relations of social control, including the adoption of personal responsibility, while leaving deeper issues of institutional vulnerability, economic divide and insecurity unaddressed; this study is, therefore, concerned with understanding Canadian consumers and clients as subjects of the overarching governmentality of neoliberalism.

According to Brown (2006), theories that consider such methods of governance have come the closest to understanding the marked significance of technology in terms of its power and control. It is the globalizing and dispersing enterprises of risk management and government-at-a-distance that have led to the decline of linear, centralized controls and transactions of personal information through various networks

(O'Malley, 1998; Brathwaite, 2000; Rose, 2000). However, Burchell (1991) notes that these theories have traditionally been criticized for over-relying on notions of social technology to the relative detriment of actual technological innovations (see also Foucault, 1991b; Garland, 1997); as such, it is important to re-examine the effects of changing technology amidst rising claims being made about IDT, paying particular attention to notions of power, responsibility and disciplinary control.

2.14 *Governing IDT*

To summarize the arguments for clarity's sake, neoliberalism and risk management strategies are intrinsically linked; citizens are increasingly expected (and agreeing) to become responsible, rational choice-makers in self-governance and self-responsibilization. The Internet has served to complicate this relation; in lieu of effective policing, consumers are expected to take heed of incessant warnings and engage in preventive action. No matter the level of responsibility of individuals, the neoliberal assumption is that responsible citizens will not reveal their information online to protect themselves against IDT. However, there exists a huge disconnect between the social construction of identity and the neoliberal restructuring of identity that fits the needs of the market economy. While government policy has encouraged individuals to protect themselves through responsible decision-making, market practices dictate that highly-valued personal information be shared and volunteered through enterprises such as online banking, responsibilizing individual users and expanding the opportunities for crimes such as IDT in the process.

The problem lies with the fact that no matter where the error, be it the corporation failing to safeguard its customers' information or the individual consumer themselves, it is the individual who is made responsible for cases of IDT—they must take it upon themselves to find out as much information as possible, act quickly to respond to incidences of IDT, maintain their innocence and convince the authorities that they abided

by all terms and conditions. Neoliberal forms of governance such as these, as ways of understanding consumer protection efforts and the multidinous forms of responsibilization within corporate legal language, become particularly salient points in cases of IDT, worthy of further examination.

CHAPTER 3

3. *Methodology*

This research project, as mentioned previously, seeks to identify how key policymakers define the meaning of IDT (including the associated risk factors/causes and proposed solutions) as well as explore the similarities and differences between the discourses mobilized by these policymakers. To answer these questions, I have analyzed the publicly available IDT policy documents published by the Consumer Measures Committee (a subcommittee of Industry Canada) and the Royal Bank of Canada. These documents are a snapshot of the discourse around identity theft. Although they arose in the context of a policymaking process, an analysis of that process is outside the purview of this study. Accordingly, the documents are analyzed as social artifacts that concretize a particular discourse at a point in time.

The Consumer Measures Committee was purposively selected because of its special status within Industry Canada, the Canadian government department with primary carriage of the IDT file[3]. The Committee, which is a multi-jurisdictional group with representatives from the federal government as well as every province and territory, is mandated with improving the marketplace for Canadians. In that capacity, it has solicited feedback from a wide group of stakeholders including businesses, all levels of government, the financial industry, credit reporting agencies, members of the public and law enforcement. As such, it is linked to policy development at all levels of government, and has established working relationships with other key players, including the financial industry.

The financial sector, including banks, insurance companies and credit reporting agencies, has been actively involved in lobbying the government with respect to IDT for

---

[3] Justice Canada is responsible for criminal legislative responses to the problem but the issue has been defined primarily as a commercial one, and Industry Canada has taken the lead on federal-provincial-territorial initiatives and public consultations dealing with potential solutions.

the past decade. Accordingly, it is a key stakeholder in the development of policy in this area. I purposively selected documents published by the Royal Bank of Canada because it is Canada's largest bank in terms of market capitalization (RBC, 2009e), and accordingly holds a premiere position amongst competing financial institutions.

Since I was interested in exploring the ways in which these policymakers construct the meaning of IDT within the public debate, I decided to conduct a qualitative analysis of IDT policy documents each institution has published or otherwise made publicly available.

3.1 Sampling Method

The documents selected for analysis are comprised of the Consumer Measures Committee's *Identity Theft Kit*, *Identity Theft Kit for Business*, discussion paper, consultation workbook and communiqués, and the Royal Bank of Canada's websites, policies, legal literature, and brochure information. All of the documents are publicly available, meaning that the research is unobtrusive by nature. The policy documents have been drawn using personal judgment for analytical appropriateness (Babbie, 2004) and do not represent any meaningful population; any conclusions that are drawn are reflective of these units alone. The documents were chosen because of their particular features or characteristics (i.e. revolving around IDT), which enabled detailed exploration and understanding of the central themes and puzzles of the research (Ritchie et al., 2003: 78). Whether these documents represent the best units for analysis is something worthy of discussion below; however, "it is easier to show how dynamic discursive practices take part in constituting and changing the social world when analyzing the reproduction and transformation of discourses across a range of texts" (Chouliaraki & Fairclough, 1999: 51). The documents include the entire range of publicly available information on IDT from the two bodies, and each text was understood as informed from "differing discourses, contending and struggling for dominance" and was understood as

the "sites of struggle and in being the sites of struggle, texts are the sites of linguistic and cultural change" (Kress, 1985: 32). The documents were understood and pieced together as a single snapshot of the IDT problem as defined by the CMC and RBC. By choosing these sample units, it is hoped that amongst the differing policy discourses forming and informing the particular documents(s), similar themes and social structures will emerge and lead to explanatory insight.

3.2 *Theoretical Model for Analysis*

Undertaking a qualitative analysis of the policy discourses contained within the documents means that the research will draw upon numerous traditions including: narrative analysis, which identifies the basic story being told and how it is constructed, the intention and the meaning of the story or plot (Reissman, 1993); and policy analysis, where analysis is targeted towards providing answers about the contexts for social policies and programs the effectiveness of their delivery and impact on social problems (Ritchie & Spencer, 1994). The application of critical thought is hoped to uncover the ways in which IDT is defined as a problem and how the CMC and RBC have constructed best-practice type solutions to the problem.

An interrelated set of texts and the practices of their production, dissemination, and reception (i.e. talking, writing, etc.) that bring an object into being (Parker, 1992; Woodilla, 1998) are understood as a discourse. Understanding discourses as the sets of meanings or representations which constitute a phenomena, the practice draws heavily on the tradition of social construction (Bloor and Bloor, 2007) which allows people and policymakers to continually create—or construct—fresh understandings about the world around them; because it is a social process, it can appropriately be termed as social construction (Berger & Luckmann, 1966). This analysis explores how the policy discourses contained within the documents of the CMC and RBC contribute to the constitution of social reality by making meaning (Philips & Brown, 1993).

The language of the documents was understood neither as transparent or reflective (a "neutral information-carrying vehicle") but rather as a site where meanings are created and changed (Taylor, 2001: 6). This required observation of the "specific meaning and relevance structure for the human beings living, acting, and thinking therein" (Schutz, 1970: 273), meaning that this research consisted of studying things in their "natural setting, attempting to make sense of, or to interpret, phenomena in terms of the meanings people bring to them" (Denzin & Lincoln, 2000: 3). Following the advice of Bryman (1988) and Potter (2004), the research was committed to understand the way versions of the world, events, and phenomena (such as IDT) are constituted as social realities within the documents.

While not new in any respect, the analytic field of discourses began, in essence, with the work of Michel Foucault. For Foucault (2002), discourses are constitutive, meaning that they have to power to construct meanings. They are also productive (Foucault, 1990; 1991b), defining and establishing truths of 'what is' and 'what is not' within texts (e.g. what is responsible action and what is not responsible action) and uniting to produce both social meanings and effects. Accordingly, the research is grounded in governmentality theory, concerning itself with how IDT has been constructed as a problem and how individuals and institutions are to conduct themselves in relation to that construction.

The goal of the research was not to provide definite answers, but to expand social understanding and highlight any controversies. Using the work of Foucault (1991b) and Joel Best (2008) as a guide, the magnitude of the IDT problem was identified first. Once the concerns were identified within, the motivations and undercurrents came to light through following a thorough process of working through, and saturating, the sampled data.

What is being attempted within this research project is not a presentation of a full (or even correct) picture of what is happening, but rather an understanding of social meanings to the problem of IDT, participant roles and the systems in place. Using the tradition of social constructionism, the research effort is concerned with the following:

1. A critical stance towards taken-for-granted knowledge and understanding
2. That our knowledge of the world is both historically and culturally specific
3. That this knowledge is created, sustained and renewed by social processes
4. That our knowledge and actions are intimately related and reflexively inform each other (Burr, 1995 cf. Rapley, 2007: 4).

Joel Best's (2008) contribution to understanding social problems through construction and claimsmaking were chosen as the main analytic frame for the research project. He claims that once situations are understood as harmful conditions, we can look around and identify various social problems (e.g. IDT = a harmful social problem), the solutions suggested and the implications

The documents were understood to have resulted from the social problems process where problems are identified, receive the necessary support, and ultimately garner the attention of policymakers, who include government agencies (e.g. CMC), schools, the private sector (e.g. RBC)—namely, those with power to decide courses of action—in addition to legislative assemblies. However, the thesis does not attempt to understand the natural history of the IDT problem , focusing instead of the meanings embedded in the documents themselves. Best (2008) notes that not all social problems fit the model, but it does help organize the thinking process. The process, according to Best (2008; fig. 1.1) moves through six stages: claimsmaking, media coverage, public reaction, policymaking (where the documents are situated), social problems work and policy outcomes.

At the very first stage, claimsmaking, a particular problem is presented as troubling and ought to be done about the social problem (e.g. identity theft). Best (2008) defines the claims as "arguments, efforts to persuade others that something is wrong, that there is a problem that needs to be solved" (18). Any social problems process, therefore, begins with a perception. The perceived problem receives support through persuasion, which features three fundamental components essential to making a claim: grounds, warrants and conclusions (Best, 1990; Toulmin, 1958). Best (2008) contends that the grounds are usually assertions of fact; that is, grounds include information and evidence about the troubling condition and usually include a typifying example (which are rarely typifying and are usually designed to elicit concern) or in Kingdon's (1984) terms a "focusing event", the name of the problem (i.e. identity theft) and a statistic (which is usually a big number since it implies a big problem and a big concern). Additional grounds are also employed to lend strength to the problem such as characterizations of a "worsening situation", a "familiar type of problem", the "kind of people affected" (Best, 2008: 34) and so on. Claims made about IDT within the policy documents, as will be seen, make great use of such devices in defining the problem of IDT and the appropriate solutions.

Once the grounds are established, there is a justification that something must be done about the troubling condition. Best (2008) defines such justifications, which explain why something ought to be done, as warrants. He adds that warrants invoke values and argue that "the condition identified in the grounds is inconsistent with what we value, and therefore we need to do something about it" (*ibid*: 36). Taking IDT in mind, the crime can be understood as violating both financial and personal values—e.g. personal wellbeing, security—requiring action on the part of governments (CMC), agencies, the private sector (RBC) and individuals.

The conclusions, then, are the specific remedies to the troubling situation; they specify what should be done and what action should be taken to address the social problem (Best, 2008: 39). These conclusions usually include both short and long-term goals, whether gathering support and making others aware of the problem or, ultimately, affecting policy change through new laws or programs (*ibid*). Once the claims are made and substantiated as *fact*, it is up to claimsmakers to ensure that their claims are being heard.

Usually, the claims come to the immediate attention of the media who tend to search for what is new and troubling in the world of news reporting. Their interest and reporting ensures that the claims reach a broader audience. Media attention usually creates new levels of concern with the public, affecting their opinion and causing them to lend support to the claims (Best, 2008) through additional calls for action. As IDT is a growing concern, it represents a prototypical social problem.

Once the claim has progressed through the first three stages (claimsmaking, media coverage, public reaction), policymakers then respond but with "their own considerations" which "shape the policies they create" (Best, 2008: 21-22). Pal (1992) contends that the policies are understood as "hypothetical solutions to the problem" (7) and necessarily include a definition of the problem as well as the policies' aims, directions and substantive meanings—Bill S-4 would be an excellent unit for further studies in IDT policy analysis as it showcases the progression from problem, policy proposals, policy work and subsequent calls for reform. It is here that the CMC and RBC policy documents' origins are understood to be. For purposes of this research, uncovering the way the problem is understood and addressed by the CMC and RBC was the primary concern as was finding a grand-narrative that informed both their understandings of the problem.

The documents available from the CMC and RBC were understood to have arisen out of this policymaking stage. Since policymakers do not have the time or money to do everything that is asked of them, they must set priorities and decide which problems need solutions now. Best (2008) notes that just as claimsmakers compete for the attention of the media and public, policymaking can be understood as a competitive process too (*ibid*). Kingdon's (1984) policy stream model elucidates understanding of how particular problems and policies (such as IDT) arrive at the top of policymakers' agendas.

There are three streams according to Kingdon's (1984) model: (1) the problem recognition stream, (2) the policy proposal stream and (3) the political stream. The problem recognition stream is recognized in the process of claimsmaking, active campaigning on behalf of the troubling condition, and bringing those conditions to the attention of the press, public and policymakers. The second stream, policy proposal, consists of specialized constructions to deal with the problem and may include broad cognitive approaches according to Best (2008). These proposals can come from various experts, think thanks, working groups, and officials; however, policy advocates must continually revise and repackage their proposals and wait until they are given the opportunity to present their proposals in a hearing. And lastly, the political stream refers to what we might think of as the current political situation—i.e. who has been elected and what beliefs and values do they favor? (Kingdon, 1984). While these streams are constantly flowing, they are understood as having minimal contact; however, there are times amidst the competition when "a particular construction of a troubling condition complements a particular policy proposal that, in turn, coincides with the current political alignments" (Best, 2008: 201) resulting in new policies or new policy proposals. Muller (1990) claims that this perspective views policies as responses to a social problem reflecting a certain social reality that has been articulated by mediators (claimsmakers,

the media, new social movements, political parties or interest groups) and then debated within a particular decision-making process (whether democratic or not). Rallying around a common enemy makes the convergence of the three streams a greater possibility, and in the case of IDT, a reality for the CMC and RBC.

Although the detailed process by which RBC or the CMC arrived at their particular policies cannot be known fully, it is reasonably assumed that the policies resulted from such convergence. This thesis cannot attempt to understand the process CMC and RBC undertook to produce their documents, but is concerned solely with the documents themselves as one of the concrete artifacts of the process. While these policies are current and up-to-date on IDT, it cannot be expected that they will remain the same; after all, the problem recognition stream is ongoing as "problems are introduced, evidence considered, solutions debated, decisions made, programs implemented, and policies evaluated" (Weiss, 1989: 98).

3.3 *The Products of Policy*

A social constructionist framework is necessarily concerned with revealing the discursive constructions that are embedded in texts as information that is less readily available to consciousness (cf. Locke, 2004: 40). These utterances often include articulations of power; Foucault's understanding of power is of particular importance in the context of policymaking. Power, according to Foucault (1980), has a productive force, meaning that it is able to constitute discourse, knowledge, bodies and subjectivities.

Van Dijk (1997: 17) offers an appropriate cognitive frame for understanding power within policy discourses; according to him, discourse, as a whole, is mostly intentional, controlled and purposeful human activity, and because there is most often a purpose to what is said, wrote or read, power relates to making others act as we wish or preventing them from acting against us. This type of power is hardly coercive, but rather

mental or suggestive, leading to a reliance on talk and text—it is in this sense that power is, perhaps, best understood as disciplinary control. After all,

> Power is control of action, which requires control of personal and social cognitions, which presupposes control of public discourse, which is possible only through special forms of access, which may in turn be based on political, economic, social, or academic power resources (position, ownership, income, knowledge, expertise, etc.)" (*ibid*: 22).

From a social constructionist standpoint, all thought can be understood as fundamentally mediated by power relations since some social problems (and their claimsmakers) receive the necessary attention from the public, the media and policymakers while other social problems are largely ignored; these constructions can never be isolated from the domain of values or removed from some form of belief system.

The social constructions that form the basis of cognition contribute to the production, reproduction and transformation of relations of domination (Fairclough, 1992: 87, cf. Chouliaraki & Fairclough, 1999). The domination need not be overt or oppressive but can operate systematically through mental processes that serve to produce, reproduce and legitimate power relations (whether in terms of personal interest or public interest) not by law but by technique, normalization, and control (Foucault, 1990).

Specifically, power and knowledge find their articulation in the form of beliefs and values and it is through these that knowledge and truth are generally enacted (Hall, 1997: 49; Foucault,1980). Becker (2004) claims that authoritative groups, privy to a more complete range of information, are able, through their control of resources and their capacity to exercise decisive agency, to make their viewpoint, recommendations and claims culturally dominant. In this way, social knowledge and social power are inextricably interlaced in what Becker (*ibid*) calls a *hierarchy of credibility*. For Foucault (1979), there can be no power relation without a correlative of knowledge, nor any knowledge that does not also presuppose and constitute power. Building upon such

understanding, Gaventa & Cornwall (2001: 321) argue that "better" (objective, rational, highly credible) knowledge will inevitably have greater influence and power. The interrelation of knowledge, power and belief is therefore crucial to understanding "how [discursive practices], events, and texts arise out of and are ideologically shaped by relations of power and struggles over power" (Fairclough, 1995: 132).

These power relations are not natural or objective – they are "artificial, socially constructed intersubjective realities" (Fowler, 1985: 61) needing to be shared; the research understands the publicly available material from the CMC and RBC as direct attempts to share those understandings of IDT as a social problem with concerned Canadian consumers and banking clients.

These realities are also historically situated, since every authoritative and political system has attempted to establish and to cultivate the belief in its own legitimacy (Weber, 1968). Bloor and Bloor (2007) add:

> It is always in the interests of the dominant elite group if the subjected group can accept their position as an ideological imperative—that is to say, if they believe that this is the way things should be or the best that things can be, if they 'accept their lot in life' as the old expression put it. Towards this end, power structures tend to be institutionalized and fixed by both customs and laws, which encourage people to behave in certain ways and identify with certain groups (85).

Accordingly, certain policies may be interpreted, not as collective actions aimed at resolving a social problem, but as simple instruments for the exercising of power and domination by one group or institution over another (Knoepfel et al., 2007). Such legitimation is accomplished in large part to language (Berger & Luckmann, 1966; van Leeuwen, 2008), and consist of socially relevant norms, goals, values and principles; these principles are then selected, combined and applied in order to foster perception, interpretation and action in social practices. Weedon (1987: 21) adds that language chosen is not an expression of unique individuality, but rather a construction of the

individual's subjectivity in socially specific ways.

Systematically, then, the policies employed by various public and private actors give "rise to formalised [sic] actions of a more or less restrictive nature that are often aimed at modifying the behavior of social groups presumed to be at the root of, or able to solve, the collective problem to be resolved (target groups) in the interest of the social groups who suffer the negative effects of the problem in question (final beneficiaries)" (Knoepfel, 2007: 24). In addition to the research goal of understanding IDT as a social problem within the policies of CMC and RBC, there is also concern with establishing whether or not the policies give rise to formalized action, and if the case, highlighting the restrictions (if any), how behavior is to be modified (if at all), and what interest may be served by such ends. In the words of Denzin (1994: 234), the research essentially aims to deconstruct and take apart the documents, expose the underlying meanings, biases, representations and preconceptions that structure the way they conceptualize IDT and exercise their power through such conceptualizations and accompanying solutions.

3.4 *Methodological Approach*

A qualitative analytic method was employed to examine a series of documents that have outlined expectations of individuals as victims, users and clients. Qualitative analysis stands opposite quantitative approaches and includes "any type of research that produces findings not arrived at by statistical procedures or other means of quantification" (Strauss & Corbin, 1998: 11). As such, the research involved no counting of terms or numerical values (as occurs in content analysis), but particular themes were identified through clustering and refined descriptive accounts.

Snape and Spencer (2003) also claim that in spite of clearly agreed upon rules or procedures for analysis, qualitative studies usually include the following as distinctive characteristics:

- In-depth and interpreted understanding of the social world;

- Samples that are small in scale and purposively selected for salience
- Data collection methods that usually involve close or in-depth contact with samples
- Very detailed, information-rich data
- Analysis open to emergent concepts and ideas and which may provide description, classification, association or further development
- Outputs tending to focus on interpreting the social meaning of phenomena (ff. Ritchie & Lewis, 2006: 3-5).

Where quantitative approaches tend to ground knowledge in positivistic terms (law-like regularities) that allow research to be carried out independently, objectively and value-free, qualitative researchers—such as Ritchie & Lewis (2006)—claim such an approach is inappropriate for the social world since that world is not governed by law-like properties, instead adopting Weber's (1968) concept of Verstehen, which involves the more intimate and empathic understanding of social constructions in terms of "its interpretive meaning to the subject" (Palys & Atchison, 2008: 9).

The raw data was managed through a process similar to that found in Spencer et al. (2003): the documents underwent an initial reading to gather basic understanding of the problem; upon second reading, initial themes and concepts were identified within the raw data, labeled and then sorted in a cross-sectional analysis. The data was then summarized into descriptive accounts in order to assign meaning to the themes and concepts, organized into memos and refined into more abstract concepts to detect patterns and cluster the themes and concepts; the data was essentially broken down into categorical themes and concepts, sorted and then pieced back together to form a narrative-type understanding to the problem of IDT. This was done in order to develop explanations to 'how' and 'why' type questions and seek applications to wider theories or policy strategies. Following the advice of Miles and Huberman (1994), simply naming and classifying the findings was understood as not enough. Rather, the research was completed to "understand the patterns, the recurrences, the *whys*" (67).

Although the process may appear linear, it was highly iterative and reflexive

having to constantly revisit the original or synthesized data to search for new clues, check assumptions and identify the underlying factors to the claims being made in the policies; the analysis developed until further reading and interpretation of the policy documents yielded no new themes. The themes that emerged were then substantiated from a thorough collection of information extracts selected as newsworthy or important to the understanding of IDT. According to the process, there was an inductive approach favored, starting with observation, progressing through categorization and conceptualization and culminating in the development of a grounded theory—theory that emerges from the research.

3.5 *A Researcher's Role in Discourse*

The research approach adopted has built upon Foucault's concept of discourses as semantic constructions of reality that serve particular interests of particular historical and/or social contexts (cf. Van Leeuwen, 2008: vii). According to Alvesson and Karreman (2000), this Foucauldian-informed work often focuses on unmasking privileges inherent in the constructions, informing their constraining effects, and often leads to studies of how grand or mega policy discourses shape social reality and constrain the actors therein which this study has also touched upon.

This thesis does not hope to upset any equilibrium that may exist between agent and agency; however, it is hoped that as a result of reading, one may be better able to see behind various policies, their implications and operations and come to a better conclusion on how the policies construct social problems and solutions. However, the version of reality put forth herein is not better than any other, and can always be cast aside through discursive struggles between other individuals or groups, but by presenting a procedural account, the research knowledge arrived at can contribute to new perspectives for public debate (*ibid*: 210). It is with this goal, of debate and questioning, in mind that the research was conducted.

Once the reveal is underway, questions relating to change and the consequences of beliefs can be answered according to Phillips and Jorgensen (2002) such as: does the discursive practice reproduce the order of discourse and contribute to the status quo or has it been transformed contributing to social change? What are the political and social consequences of the practice? Does the practice conceal or strengthen unequal power relations? What are the implications, both short term and long term, of the policy?

Understanding the claims, warrants and justifications to address the social problem of IDT was the driving force in directing the research into a policy analysis instead of a critical discourse analysis (focusing on the actual linguistics) or a content analysis (focusing on counting and categorizing). The research aims to understand IDT as a narrative and seeks to understand the individual implications for consumers and clients in the construction of the IDT problem and the recommended solutions.

3.6 *Reliability/Validity*

The chosen sample, theoretical model and methodological approach do not escape criticism. Firstly, engaging in a qualitative analysis runs the risk of simplifying issues for the sake of facility of observation. However, where validity and reliability are understood as measuring what was intended and measuring in such a way to be able to replicate findings, the theoretical framework of social construction maintains that there cannot be one objective truth but rather multiple and sometimes contradictory truths or versions to understanding a particular social problem. After all, a social construction analysis is deeply committed to the "view that what we take to be objective knowledge and truth is [actually] the result of perspective" (Schwandt, 1994: 125). I am confident that the findings arrived at through the research process contribute to better understanding of the problem and offer *one* valid and reliable measure of its conclusions. Although the findings may not provide a complete picture, they do offer one

insight and one perspective that should further the understanding of IDT as a social problem.

The policies found with RBC may not be indicative of those found for other financial institutions, limiting the ability of the research to generalize its findings. The policies of the RBC, or even the CMC for that matter, provide interesting analysis but cannot be understood as similar to those employed by other institutions, private or public. Conducting a micro-analysis of the documents and trying to apply any findings to a larger scale is problematic for traditionalists as they are thought to be too small to permit generalization of results beyond the sample; however, the goal is to ground the analysis in particular concrete instances, understood as occasioned and contextualized (Wood & Kroger, 2000: 76) and generate thick description (Geertz, 1973); because the process of qualitative analysis makes profound use of both time and labor, restricting the sample size was a necessary step toward saturating the data.

Also, because there was no true experiment design used, the findings of any qualitative research project will be difficult to reproduce. This represents a serious threat to inter-observer reliability and especially to attribution. What must be acknowledged is the research's own limitations in establishing cause and effect relations. As qualitative analysis is still a matter of (provisional and contextualized) interpretation, there can be no direct attributions made. Rather, the reliability and validity of the research will rely on the force and logic of the arguments; even the most persuasive of arguments are subject to their own reinterpretation and deconstruction, especially in the case of changing social meanings and their contexts. Therefore, the validity of the findings will depend heavily on the quality of argument and the particular process employed.

Since the research was conducted with a particular aim in mind (understanding the problem of IDT as a social construction), a strict chain of evidence was maintained to substantiate any findings and support any conclusions (Yin, 1989). Cataloguing

particular themes within the policies with substantial evidence will help pinpoint how exactly the conclusions were drawn, aid in convincing the reader, and help improve inter-rater reliability.

Using these documents to analyze and draw conclusions calls into account the researcher's own bias. Looking for specific answers or correlations between unrelated concepts is easier when the researcher is in a position to read into the language as they wish. However, by categorizing themes, keeping multiple sources in mind, maintaining a strict chain of evidence, and by engaging in a step-by-step process, using specific and clear language to spell out the themes, interrelationships, discursive strategies and techniques, reliability and persuasiveness of the research can be improved.

CHAPTER 4 *Data Findings and Analysis from Consumer Measures Committee*

4.1 The Sample

This chapter presents the findings from employing a qualitative analysis of publicly available documents of the Consumer Measures Committee (CMC) on the issue of identity theft. The documents include the *Consumer Identity Theft Kit*, *Identity Theft Kit for Business*, discussion paper, consultation workbook, and the communiqués/press releases available (CMC documents).[4]

The *Consumer Identity Theft Kit* (2005a) contains three sections: informational material on identity theft and helpful tips to guard against it (numbering ten pages), frequently asked questions (two pages), and the Identity Theft Statement itself (seven pages).

The *Identity Theft Kit for Business* (2005b) is "intended to emphasize the need for effective personal information policies and practices" (pg. iii), and discusses IDT as a concern for business (which totals four pages). It also contains tips to reduce the risk of data breaches (numbering eight pages), information about what to do when a thief strikes (three pages), and tools to employ in the event of theft (four pages). The entire business kit totals eighteen pages.

The discussion paper, *Working Together to Prevent Identity Theft* (2005c), is divided into four sections: an overview of the problem posed by IDT (amounting to little more than a page); a discussion of why IDT is a growing problem and who can help contribute to a solution (roughly two pages in length); an overview of current legislative frameworks in Canada and the U.S. (two and a half pages); specific options for legal reforms to combat the problem (fifteen pages); and finally, concluding remarks (half a

---

[4]Of note, the communiqués from the provinces of Ontario and Quebec, both dated July 6, 2005, were presented with a URL link on CMC's website; however, upon following the link, both pages resulted in a "404 Error: Page Not Found" / "Fichier Non Trouve" – these communiqués have subsequently been removed from the website.

page). The paper totals twenty-eight pages including references. The discussion paper was released on July 6th, 2005 as part of a public consultation on measures to address IDT, and solicited views from both the private sector and public on the policy and practical implications of the issues raised in the paper.

The discussion paper is accompanied by a consultation workbook (totaling twenty-one pages) which includes a list of specific legal reform proposals along with specific questions (e.g. "Do you think this option [truncating payment card numbers, as one example] would better protect against identity theft? Why or Why Not?"). Both the discussion paper and consultation workbook include a briefing note at the beginning of each document, respectively, explaining why CMC is requesting "recommendations for the best framework for combating identity theft – irrespective of the short-term costs and benefits for various industry players or consumer groups" (CMC, 2005d: 3). The recommendations were then evaluated by CMC and either included in or excluded from CMC's policy guidelines to consumers, businesses and government at their discretion.

Lastly, the sample includes the six communiqués posted on CMC's website, from 1998 to 2007. One is dated 1998, one is dated 2001, one is dated 2004, two are dated 2005 (a day apart, and immediately following the discussion paper's completion on July 5), and one is dated 2007. All of the communiqués are news releases, except the last, which is a copy of remarks Michael Jenkins made to the House Standing Committee on Access to Information, Privacy and Ethics made in Ottawa on May 10, 2007.

4.2 *Findings*

The following section summarizes my analysis of the aforementioned CMC documents. I begin by outlining the definition of identity theft (IDT) within the documents, exploring the ways in which it is conceptualized and discussing how it happens and the consequences thereof. I then examine five other themes found within the CMC sample:

(1) CMC as "partner"; (2) CMC as "educator"; (3) the importance of "trust"; (4) and the individual as "cause" of IDT.

4.2a *CMC's Understanding of Identity Theft*

CMC documents, as a whole, identify IDT as a "national concern" (CMC, 1998); the *Identity Theft Kit for Business* lists IDT as the "fastest growing crime that business, consumers and governments face" (CMC, 2005b: 1), while one communiqué claims that it is "increasing across the continent" (2005e: 1). CMC notes that reporting of incidences of IDT increased from 4 000 cases in 1999 to over 24 000 cases in 2002, representing a 500 percent increase and lending evidence to the difference in IDT's scale (2004d: 6) according to CMC. Additionally, a CMC press release quotes surveys that indicate that approximately 3 percent of surveyed Canadians and Americans were victims of IDT in 2003 alone, translating into a raw figure of 900 000 Canadian victims (2005e). These are the only statistics provided in the materials; all of the documents rely elsewhere on general phrases such as "serious consumer concern" and "increasing across the continent" (2005d) to underscore the extent of the crime.

Despite the increases in reporting, media coverage and general concern, CMC's discussion paper (2005d) claims that "there is a great deal of confusion about what the term 'identity theft' means" (pg. 5), and likens the concept of IDT to a "puzzle" (pg. 8). To solve the puzzle, CMC's paper attempts to clarify the meaning of the term given the "gaps in the Criminal Code and other initiatives currently underway in the federal government" (*ibid*: 5), and in doing so, positions the CMC as a legitimate 'authority' who 'knows' what identity theft is and is able to communicate its privileged understanding of the crime to uninformed Canadians.

The *Consumer Identity Theft Kit* defines IDT as a crime that occurs "when someone uses your personal information without your knowledge or consent to commit a crime, such as fraud, theft or forgery" (CMC, 2005a: 2; see also CMC, 2005b: 2). This

first definition places the consumer, the "you" in the sentence, in the role of victim; IDT is therefore understood to be a direct action taken against the individual consumer. CMC adds, "identity thieves steal key pieces of personal information and use it to impersonate you and commit crimes in your name" (*ibid*). The use of the active voice (i.e. the object receives the action of the subject, as in "thieves steal information") places the emphasis on "your" information; keeping your information safe and secure from motivated thieves and incidences of identity theft, then, is—or should be—of paramount importance to you. This suggests that each reader has a personal interest in doing something to deal with the problem before it personally affects him or her, characteristic of a typical social problem according to Best (2008).

While the kits define IDT in terms of *use*, the discussion paper (2005d) notes that IDT may also involve the acquisition of personal information, i.e. the acquisition or transfer of personal information as an instrument to commit crimes in the future (*ibid*: 5). According to the *Consumer Identity Theft Kit,* identity thieves typically acquire the personal information required for IDT by way of the following:

- Stealing information from victim's wallets, purses, homes, vehicles, computers, personal electronic devices (laptops, PDAs, iPods), mailboxes or recycling bins
- Posing as trusted officials of companies, law enforcement
- Tampering with ABMS or point-of-sale terminals to record PINs and account info
- "Phishing", using computer spyware, viruses and Trojans (2005a: 3)

CMC claims that identity thieves' propensity to acquire the requisite information and not use it immediately thereafter is important to understand. The CMC claims that IDT is "not always committed for its own sake" and is "commonly committed to further other criminal activity" (2005d: 6), suggesting that the continued threat of information misuse requires the individual to monitor their finances for future activity, making the "threat" ongoing and amorphous rather than defined. Since CMC also claims that thieves can steal information from public sources such as newspapers, phonebooks and public records

(i.e. certifications) (CMC, 2005a: 3), the consumer is placed further in a continuing position as (potential) victim, requiring constant vigilance to quell the ongoing fear.

The discussion paper explicitly recognizes the importance of understanding IDT as both the acquisition and the use of personal information, highlighting the fact that doing so "allows [the CMC] to address the problem as a whole – from the collection of information to its distribution, misuse and correction – and identify measures, which can mitigate the harm to the consumer" (CMC, 2005d: 5). From this perspective, IDT is presented as a multi-stage issue, and CMC is the expert problem solver and beneficent overseer, cognizant that IDT may occur at each and every stage of the information-lifecycle. IDT is characterized in individual terms, caused by individual fault rather than systemic flaw. CMC does acknowledge that "corporate practices contribute to the problem" (*ibid*: 6) but limits their evidence of such practices, within the discussion paper, to employees who accept bribes, pilfer information on behalf of organized crime or unwittingly release personal information to criminals posing as legitimate businesses. Rather than acknowledging the loopholes that allow criminals in, the CMC documents focus on individual, micro-level solutions that will mitigate, rather than eliminate, potential harm.

CMC's definition of IDT within its *Identity Theft Kit for Business* (CMC, 2005b) is focused on understanding the concept vis-à-vis business practices and data management; however, CMC fails to note that since IDT is something that happens to specific individual victims, corporations and businesses cannot technically suffer from the phenomenon but can only suffer from data breaches, mismanagement, and 'inside jobs' that will lead to IDT of their clients; consequently, one of the documents (2005b) provided by CMC can actually be considered a misnomer. In making the document about IDT, the CMC has also positioned corporations as victims, collectively suffering egregious damages as a result of individual action taken by employees ("insiders") and

identity thieves. Using IDT in the title, rather than data mismanagement, diverts blame away from the corporation as the entity that creates the loophole and onto the thief who exploits the loophole for criminal purposes.

CMC situates IDT within the new information marketplace to address "the more fundamental questions of how technology as well as business practice as a whole unwittingly facilitate fraud" (2005d: 5). The marketplace is described commonly within other CMC texts as: "borderless", "expanding", "increasingly open", "evolving", "ever" and "rapidly changing" on a "daily" basis, "more complex" and "larger" than ever before (see CMC, 1998; 2001; 2004). Yet it is the discussion paper that claims:

> New information technologies have revolutionized business practices and made Canadian companies more efficient and competitive. However, the electronic collection and storage of personal information has, at the same time, multiplied the risk that personal information may be misappropriated and used to commit fraud and other crimes. This is called 'identity theft'" (CMC, 2005d: 2)

The exponential and uncontrollable advances in technology and corporate practices—of which PINs, ABMs, online banking, Interac and the expanded use of SIN are immediately listed (*ibid*)—are understood as foundational constructs granting thieves the opportunities to commit IDT and within which the social meaning of IDT takes shape as an unforeseen consequence of technological progress. According to one of CMC's communiqués (2001), the business kit (2005b) and discussion paper (2005d), global market forces such as quick access to and overreliance on credit, ultra-competitive prices and greater product choice as well as information-sharing initiatives, have made IDT that much easier a crime to commit since personal information is being communicated more often and inside jobs are on the rise. This claim is directed primarily at businesses themselves, appearing in the consult/discussion paper and the kit, and serves as motivation for taking proactive measures against individual culprits who will exploit the system if given the opportunity.

According to the information above, CMC sees a greater need for consumers to identify the associated risks and "have the information and skills needed to participate effectively in today's marketplace" (*ibid*: 1). In order to uphold its mandate "to facilitate the process for reconciliation of consumer related measures and standards" (CMC, 2007: 1), CMC has and continues to actively develop consumer education initiatives "with a view to protecting consumers and informing them so that they can better protect themselves" (*ibid)*. According to CMC, all of their efforts are carried out with this purpose, placing them as an effective guardian of sorts, disseminating the necessary information to those unable to protect themselves on their own accord. These educative efforts have been undertaken since identity thieves have "adapted to new technologies and practices at a considerably faster rate than enforcement or legislative agencies" (2005d: 26), characterizing the individual consumer as the best-line of defense. Taking this as a particular salient point in relation to CMC's understanding of IDT, the consumer is socially understood as unable to guard against IDT without proper guidance and instruction; CMC's presence and knowledge, on behalf of concerned Canadians, is therefore legitimated and welcomed in light of such characterizations.

In communicating their understanding of IDT, CMC positions the consumer in a position of need since "consumer behavior can put individuals at risk (CMC, 2005d: 6). Because most of the useful information (and tips) presented within the available texts is for the individual consumer's benefit, they (or "you" as previously mentioned) may be understood as the crucial piece in prevention and the most-immediate solution.

4.2b *CMC As Partner*

Throughout the documents, CMC repeatedly underlines the need for cooperation between many actors in the public and the private sectors (CMC, 2007: 4) and the fact that "all have a role to play" in making sure personal information is not available to identity thieves (2005d: 7). According to one of CMC's communiqués (2005e), a

partnered approach is understood as both necessary and critical to maintaining market efficiency and guarding against IDT. Words frequently used within the documents to characterize this mutuality include "shared responsibility", "cooperation", "coordinated" or "collaborative action", "cooperative enforcement" or "initiative", and "partnership project" among others. Such phrases emphasize the need to work together, and this interdependence and shared responsibility emerges as an objective reality of dealing with IDT.

Those who are "working together" to address this "continuing challenge" are recognized by CMC as part of a "multi-stakeholder group" (CMC, 2001). To steer the group, CMC assumes the role of identifying and defining the problem, proposing solutions and helping the stakeholders do what is necessary; doing so positions the CMC to "set priorities for collaborative action" and "better intergovernmental cooperation" (CMC, 1998; 2001) in order to put scam artists "out of business" (CMC, 1998: 2). The texts present CMC in a privileged position with regards to knowledge and expertise, promoting liberal discourses so that all may enjoy maximum benefits and protection from the marketplace. CMC is constructed, largely through expository language, as being an active force, working on behalf of Canadians and employing a number of different pieces of legislation—*PIPEDA*, the *Bank Act*, and the *Criminal Code* among others (CMC, 2005d)—towards a singular purpose. However, this presents an oversimplified picture of IDT as a problem that must be managed through the individual rather than solved entirely—individuals are to be afforded additional protections from government and must receive better education on how to better prevent incidences of IDT. As seen below, managing IDT in such a manner positions businesses as victims of identity thieves and criminal "insiders" as opposed to those who create, use and expand the systems identity thieves exploit and, thereby, allow IDT to continue to grow exponentially.

The sample represents CMC as actively engaged in measures to improve the current situation including, but not limited to: the *Canadian Code of Practice in Electronic Commerce*, praised as an "outstanding example"; and *Fraud Prevention Month*, a campaign CMC uses in order to distribute its educational products to public and police (CMC, 1998; 2007). It is noted that CMC initiated public consultations in developing its *Consumer Identity Theft Kit (2005a)* and *Identity Theft Kit for Business* (2005b), again characterizing CMC as a hub around which the multi-sectoral cooperation takes place.

Just as prevention of IDT is understood as being the responsibility of many actors, responding to the crime is something that also requires close co-operation. The *Consumer Identity Theft Kit* implicates the individual consumer as one of the key partners required to effectively respond to IDT yet reduces their role to one of reporting. By reporting the crime immediately upon detection (to banks, police, CRAs, 1-800-O-CANADA, Canada Post, Privacy Commissioner of Canada, Phonebusters, businesses providing the thief with credit or goods, etc.), victims can "minimize the damage and help prevent any further fraud or theft" (*ibid*: 8). Businesses will then have the information required to assume a savior role, able to offer to the victims the resolution (i.e. new documentation, reimbursed money) they seek once they complete their own investigations. While waiting to be saved, victims are to "be sure to record the steps you've taken to report the fraudulent use of your identity" (*ibid*: 8), and sit and wait patiently for the response to come to them. Required reporting furthers the conceptualization of IDT as a broad-ranging social problem yet reinforces the unequal power relations between the individual (those needing assistance) and the agencies (the saviors).

Reporting the incident is made simpler by using the CMC-provided *Identity Theft Statement*; the statement, contained within the consumer information kit, is designed to help victims notify affected parties and give them the information they need (CMC,

2005a; 2007), setting the CMC up as a rescuer to consumers who do not know how to properly report the problem to affected stakeholders. It is made clear that companies require victim information and any additional information they deem necessary in order to investigate and institute corrective action. The interplay, here, is of particular interest as it draws upon a mutual coordination when gathering the required information, yet implies that the agency is the only one capable of saving consumers from the "staggering and permanent effects" (CMC, 2005b: 12) that come from IDT.

Instead of reinventing the wheel and addressing the underlying weaknesses that grant identity thieves the means to commit the crime so easily, CMC documents (2005a; 2005b) work towards explaining IDT as an individual problem, calling on readers (consumers, business owners/managers) to ask themselves what they can do to solve (or respond to) the problem of IDT rather than asking what needs to change. In spite of the partnered approach, CMC documents suggest that, above all else, IDT is a harm that befalls individual consumers and businesses rather than a broad-ranging social and systemic problem (and unforeseen consequence) of the emerging electronic marketplace.

4.2c *CMC as Educator*

While the need for partnered prevention is evident within the CMC literature, there is a greater focus on teaching both individuals and businesses how to prevent IDT from happening and how to respond to it when it does. The narrative in the documents regarding the need to bridge "gaps" in understanding IDT (CMC, 2004) implies there is a natural tendency for consumers and businesses in a knowledge-based economy to engage in risky behaviors simply because of their own ignorance. Accordingly, the CMC's information kits provide the necessary access to information and expert advice to

both consumers and businesses, each of which will be discussed, in order to fit their respective behaviors into the needs of today's market economy.[5]

Educating Consumers

Information presented within the *Identity Theft Kit* (2005a) takes the form of consumer tips, frequently asked questions that consumers may have, and tools that victims can use to help streamline the process. Headings found therein include the following: "signs your identity might have been stolen"; "why should you be concerned about identity theft?"; "watch your identity"; and "what to do if it happens to you" (*ibid*). Information has been organized in a manner that would suggest the following: (a) you, the consumer, need to be concerned with identity theft; (b) you may not even know you are a victim and need to find out if you are or have been; (c) you need to continually monitor your situation; and finally, (d) you should heed the advice volunteered by CMC in both preventing and responding incidences.

Signs that your identity might have been stolen include: banks or creditors contacting you about suspicious transactions or unknown debts, denial of credit for reasons you cannot understand, unknown purchases or withdrawals appearing on your statements, missing or late-arriving mail (CMC, 2005a: 2-3). Additionally, victims do not realize they have been victims of IDT until they try to apply for new credit, jobs or loans (*ibid*), constructing IDT as a crime that can and does occur discreetly and surreptitiously, requiring one's careful monitoring and strong vigilance.

In spite of understanding IDT as a shared responsibility, it is the consumer victim who is identified as the one with the most to lose (both in monetary and non-monetary terms). Under the heading "Understanding the Problem" (2005d: 6), CMC claims that it is the individual victim who will "spend many hours trying to clear their names and suffer emotional anguish throughout the process" (*ibid*: 7). In addition to monetary loss, CMC

[5] CMC (2007) reveals more details on CMC's operations and focus

also claims the victim may also experience emotional damage, loss of reputation, and potential court judgments, painting the victim as the party most affected by IDT and illustrating individual consequences of IDT.

In order to guard against such potentialities, the consumer is given information and tips on "What You Can Do" in the *Identity Theft Kit* to "reduce your risk" of IDT without altogether preventing it (CMC, 2005a: 4). Tips found in this section and amongst other materials (e.g. CMC, 2005d) can be classified according to general themes: limiting one's exposure; paying greater attention to financial details; and guarding one's electronic information (*ibid*: 4-7).

The sample (2005a: 4-7) implies that there is an acceptable level of exposure that you must accept to participate in today's marketplace (e.g. carrying ID, using your PIN number with debit transactions), but, at the same time, there is a stated concern that it is individual consumers themselves who are exposing themselves to dangerous levels (e.g. carrying too much ID, not shielding their PINs from "shoulder-surfers"), increasing the likelihood and extent of IDT harm to individuals themselves, businesses and market efficiency if that information falls into the wrong individual's hands. As such, the responsibility falls on consumers, who are positioned as both victims and cause, to "pay attention" to oft-overlooked financial details, by continually monitoring their records (i.e. bank statements, credit reports) to ensure transaction accuracy (CMC, 2005a: 4). Constructing IDT as a problem of improper disclosure or inattentiveness puts the focus back on the individual and the need to ensure that they engage in safe measures.

In addition to these common sense tips, the consumer is educated about newer technological traps into which they can fall. For example, consumers are instructed to create "unique combination" passwords and install antivirus and anti-spyware software

to clear one's Internet cache, temporary files and cookies on a regular basis,[6] implying that the consumer does not know how best to protect their computer and electronic information. In highlighting how consumers are to act, respond to new threats and monitor their behaviors, CMC assumes the role of expert facilitator and teacher, helping the individual achieve levels of protection they otherwise are unable to attain. In light of the recommendations, it is the individuals' duty to listen to teacher's instructions, do what they are told or suffer the consequences of their own ignorance.

At the same time that the CMC documents provide detailed information on how to prevent IDT from happening, they also quietly acknowledge that it will strike nonetheless by providing a "What to do" section within the kit (CMC, 2005a: 8). Within the section, the first duty of individuals is to "Report it!" (*ibid*); however, the documents do not make this reporting duty easy. For example, they do not refer the consumer to one main point of contact, instead listing the multitude of organizations that could and should be contacted depending on what type of information was stolen, what the individual's particular concerns are, and if that person is concerned about future incidences from happening to either themselves or to other Canadians. The information provided claims that swift and certain reporting must be employed by the victim in order to begin the response but fails to provide unified direction to such reporting, instead opting for four separate routes.[7] In listing banks, CRAs and direct businesses as the first points of contact, CMC places importance on the immediate and tangible financial losses rather than the long-term consequences of data misappropriation. CMC gives individuals a roadmap to IDT and warns that they will be castigated when they fail to follow directions. Corporations, as will be seen, are given the option to enter into

---

[6] For full details on suggested tips, see CMC, 2005a: 6-7

[7] The highlighted routes include (1) affected banks and businesses to ensure individuals are not held liable and affected accounts are closed; (2) Phonebusters for reporting purposes; (3) the Privacy Commissioner for managing one's personal information more strictly; and (4) provincial government departments responsible for reissuing identification (see CMC, 2005a: 8).

partnerships, drawing upon mutual assistance when and where they see fit. The individual is not afforded this luxury, having to appeal to higher authorities to save them from the pitfalls of IDT. Instead of strictly regulating the pitfalls, CMC beckons the individual to act in keeping with CMC's expert teachings.

Educating Businesses

The *Identity Theft Kit for Business* (2005b) is designed to emphasize the "need for effective personal information policies and practices" conducted by the businesses (pg. iii). The information provided need not be followed; CMC claims that "nothing in this kit should be construed as legal advice," and only offers the information and tips as "general information" (*ibid*) on effective business practices. The kit focuses on generating awareness of how businesses may contribute to the causes of IDT, and provides information on best information practices to keep businesses protected against cases of data mismanagement, breaches and inside jobs.

Entrusted with the personal information of their customers, the onus is on businesses to bolster "consumer confidence and goodwill" in their practices or risk peril to their "bottom lines" (CMC, 2005b: 3), illustrating another threat of IDT but of a different sort. CMC reminds businesses that consumers are increasingly buying goods and services from suppliers outside their jurisdiction, making it relatively easy for them to "take their business elsewhere" (*ibid*: 7) if the integrity of their information is compromised (*ibid*: 1); in making this point known, CMC uses competitiveness and profitability as driving forces to follow the identified best-practices. While the business kit is offered as general information, the information and warnings contained therein actually reveal a hard-sell. CMC is portrayed as the expert facilitator, drawing upon privacy principles of *PIPEDA* within the kit (2005b) and using their own particular knowledge-claims to warn individual business owners and managers that it is in their best interest to follow the advice or risk losing money, consumer confidence and peace

of mind. With this in mind, the information still does not amount to "legal" advice but rather amounts to hard-edged, financial advice that must be followed to avoid dire consequences.

Safe and effective business practices cover information lifecycle from collection, through use, disclosure, security and storage culminating in the information's disposal (CMC, 2005b: 4-11). The tips range from the seemingly obvious—e.g. "if you don't need it, don't collect it", "if you keep it, physically secure it"—to more specific, borderline pedantic practices—e.g. "do not copy whole databases to devices when a partial list will do", buy "cross-cut shredders" as opposed to other shredders, install a company-monitored alarm system not a remote-alarm. Although intended as general information, the practices mentioned offer step-by-step solutions for businesses that border on being pedantic. For example, instead of simply destroying unnecessary information, businesses are to establish timelines for retention of data and destroy the data accordingly by removing all electronic copies, purchasing scrubbing-software, physically destroying it or hiring a company specializing in destroying information and equipment (CMC, 2005b: 10).

The tips construct IDT as a problem of information management for businesses that can be solved by following data protection principles provided by CMC and covered elsewhere in *PIPEDA*. Constructing the crime in such a manner deflects attention away from the earlier discussion of businesses actually causing the problem (where their information and corporate practices may unwittingly lead to incidences of data breach and subsequent IDT); according to the information contained within CMC's business-focused texts, businesses now simply have to secure and protect the information given to them by trusting clients against threats to customer data, both internal and external. The choice of words employed within the text indicating information businesses may not need (whether full databases or full information of clients), implies that businesses *do*

need to collect some personal information to operate effectively in the marketplace of today, and legitimizes the cooptation of personal information as a business commodity warranting sound protection.

CMC quietly acknowledges that there will inevitably be cases of data breach or mismanagement within businesses (leading to IDT) whether or not the suggested practices are followed; this parallels the admission in the consumer kit (2005a) that individuals will not be able to fully protect themselves against the threat. In similar fashion, the *Identity Theft Kit for Business* (2005b: 12) includes a section detailing "What to Do When a Thief Strikes." The section highlights the need to act quickly as the most important factor in dealing with such incidences and is reiterated throughout the section (*ibid*). The "need" to act quickly and network with law enforcement, other businesses, CRAs, government agencies or even the media *can*, according to information, help reduce damage by informing affected customers as soon as possible and help the business itself uphold its reputation amongst those affected (*ibid*). However, the size of the network should be relative to the number of affected individuals, revealing a distinction between large and small breaches, those requiring additional expertise/assistance from other organizations and those that can be dealt with directly with the client. A small breach would then, effectively, keep the incident under-wraps and unbeknownst to other agencies, and prevent accurate statistics from forming (which is a huge concern according to the presented literature and a major obstacle in understanding the total number of people affected by IDT in a given year). Reporting the incident, then, is constructed by the CMC within their policies as an option for businesses to consider, not a necessity. This is quite different from the position of individual consumers must defer to various agencies, report the incident and wait for the resolution to come to them.

The information provided for both the consumer and the business reveals the various gaps CMC sees as important in "bridging." CMC materials teach individuals how IDT happens, how best to prevent it, how to respond when the precautions fail and why it is important to heed the advice of CMC; businesses, on the other hand, are taught effective business and data management practices, in keeping with existing legislation, that will serve to reduce their risks, protect customer information and produce a healthy rate of return.

4.2d *Who Can and Cannot be Trusted*

The communiqués reiterate the fact that CMC is operating on behalf of concerned Canadian citizens. Working to improve "consumer information and protection in a borderless marketplace" (CMC, 1998: 1), the CMC's direct actions have created more "reliable consumer information", "information-sharing initiatives", and "harmonized regulations" (CMC, 2001); meanwhile, CMC has also promoted their image as an expert facilitator, enabling and assisting in IDT prevention; because they have made IDT prevention that much smoother and easier, they are seen as deserving of consumer confidence and are doing what needs to be done to effectively deal with the problem of IDT.

The documents provided by CMC stress the need to create trust in the marketplace and individual businesses; CMC presents various initiatives to demonstrate to consumers that they can and should trust in the marketplace—since CMC is effectively working for Canadian consumers to ensure their safety through effective policy proposals and promoting best-practices along the way. CMC positions itself as an effective oversight committee, ensuring that consumers are afforded the additional protections they need in order to stay safe in a healthy, efficient marketplace.

In spite of its guardianship, CMC admits that the risk of harm from IDT cannot be eliminated fully and that there is an inherent flaw in the market that allows this kind of

crime to flourish, plotting individual practice against systemic failure. The CMC, as a legitimated authority on the topic, has provided various policy options that have improved market and enforcement regulations, but at the same time, has also shifted the problem of IDT to the individual.

A continuum of trust emerges within CMC documents which consumers must be able to recognize to effectively guard against IDT. The documents tell consumers what to look for in reputable companies; "reputable companies" should, according to information provided by CMC (2005a, 2005b), have systems in place at five distinct stages—as listed above in "Information Designed for Businesses"—to increase or bolster consumer confidence and trust and maintain a policy of "openness" (CMC, 2005b: 8). Further, CMC notes that there will be those companies who take additional measures, over and above what is required of them, to ensure clients enjoy added benefits and privileges and that seeking those companies out should be relatively easy given the information and characteristics they, the CMC, provide. As such, a continuum of trust emerges within the sample with CMC poised at the top, followed by reputable businesses in which trust may also be placed.

The sample provides concrete examples of CMC's contributions to a safer consumer environment (Fraud Prevention Month is but one example[8]), its goals and commitments to the Canadian people, detailed instructions on how to distinguish the reputable business from the irresponsible. In doing so, the CMC effectively tells consumers there is trust to be had in the information CMC offers, the technologies and marketplace if they follow the directives outlined. CMC's "determination to take action" and "set priorities" (CMC, 1998; 2001) on consumer safety issues such as IDT has resulted in direct action and sound information consumers can bank on, increasing their own safety and reducing the risk of IDT by following the trusted advice of the CMC,

[8] For further examples of CMC's contributions, refer to the communiqué dated 2007.

recognizing CMC's reputation for putting consumers first and, ultimately, pinpointing the reputable companies with whom consumers can interact with confidence.

However, within this rhetoric, there is an underlying assumption that IDT is caused by the consumer. Within the sample, there appears to be a marked attempt on the part of the CMC to highlight the consumer faults criminals have exploited including but not limited to: taking information from one's mail, wallet, purse, home, vehicle, computer, PEDs or tampering with ABMs (CMC, 2005a: 3-6). In highlighting those areas that require heightened awareness and renewed vigilance (over what information consumers carry, the importance of said information, etc.), the personal-policy recommendations of the CMC indicate both past and present consumer faults in guarding these areas, reasons why responsible behavior cannot be taken as a given, and justifications for bringing consumers more reliable and complete information. Because there is little to no impact on trying to decrease the overall numbers of motivated identity thieves, listing the areas for concern indicates the greatest tool inherent in CMC's policy documents: better information to those who needed it previously and those who need it now.

In cases of IDT when the consumer is found to have failed to abide by expectation or obligation, it is the consumer who is held responsible; more specifically, the consumer is regularly suspected and subsequently understood to have failed in living up to expectation and allowing the identity thief easier access to their information. To guard against such cases, CMC information aims to inform consumers, so that they may be better protected *in* knowledge. As noted within the "need to educate", CMC discourses recognize the "urgent need" (CMC, 2001: 4) to bring consumers more and better information, or "the most reliable and complete information" (CMC, 2004: 1) to ensure that they are better informed and better able to defend their interests (CMC, 2001: 1). CMC documents reveal that corporations that play by the rules, i.e. PIPEDA

and similar privacy legislation, are trustworthy, but the consumers who use and rely on their services, having little or no choice in the matter (i.e. if a loan is needed, then personal information must be given), cannot be trusted since they take unnecessary risks, and are ignorant of criminal methods and prone to common errors. The pressing "need" indicates a previous deficit in knowledge: that consumers do not know the proper way to interact through the market, are prone to dangerous and risky activities that unknowingly expose themselves to identity thieves and are, therefore, initially undeserving of trust when it comes to preventing IDT. This reluctance to grant trust to consumers is made clear by CMC's reminder that the consumer can and will be subject to businesses' own investigations (see CMC, 2005a). Accordingly, then, the consumer is placed well behind CMC and businesses along a trust continuum. Their behaviors are to be monitored and investigated, and ultimately, transformed through various mechanisms, many of which are found within the consumer kit (2005a). Consumers are to be made more aware of, adhere to and internalize the principles maintained within CMC's policies if they wish to become responsible consumers deserving of increased trust.

The consumer kit (2005a) reveals a number of consumer tendencies that are classified as causal contributors to IDT including: sharing personal information to those believed to be trustworthy (pg. 4); regularly choosing convenient rather than secure passwords (pg. 6); failing to secure personal information (pg. 4 & 7); and typically being slow to react to suspicious activity, essentially acquiescing to the crime (pg. 5, 8, 9, 11). CMC's accounts of typical individual faults characterize the consumer as naïve, carefree, lazy and uninformed—ultimately as cause to incidences of IDT; however, the tips and practices preached by CMC are provided with the purpose of replacing these natural consumer tendencies with heightened responsibility, prudence and diligence in keeping with the needs of the marketplace.

Just as the consumer is suspected (and understood) to have caused incidences of IDT, CMC's business kit (2005b) reveals individual *employees* cause data breaches and subsequent IDT. Therefore employees are also undeserving of trust. According to CMC's *Identity Theft Kit for Business* (2005b: 7-8), untrustworthy employees are those who: do not use unique passwords or change them regularly (every 90 days); disclose information to thieves posing as trusted officials/creditors; and fail to secure personal information whether by lock and key or password. From this perspective, IDT or data breaches can be directly traced to personal fault, not systemic flaw, bestowing culpability on those who do not abide by good business practice. In light of such risks, the employee, according to the material (2005b: 10), should not be immediately trusted and must be kept under constant surveillance.

Furthermore, since these employees have the necessary access to commit IDT, they are potential thieves[9]. CMC, therefore, suggests that businesses "limit access" to a "need-to-know" basis, allow only the system administrator to complete network tasks, and should "check logging data and audit trails for unusually or suspicious activity", e.g. employees accessing information irrelevant to their daily tasks (2005b: 7). Employees must also be screened regularly to ensure they remain "free of criminal records" (*ibid*: 10), again labeling employees as potential criminals. CMC strips incidences of data breaches down to the level of individual perpetrators and effectively grants reputable companies the ability to save face, protect their company image and retain the confidence of their clients by claiming to be yet another victim of IDT and inside jobs.

The knowledge claims provided by CMC characterize individual consumers and employees as the weak links in guarding against IDT. According to the CMC, consumers

---

[9] CMC offers a typifying example of the damage that can be caused by a rogue employee, who had been copying debit card information as he swiped customers' cards, amounting to over $200,000 in losses. That employee was eventually caught and was charged with 178 charges of fraud (CMC, 2005b: 3).

cannot be initially trusted to guard against IDT—they are described as mistake-prone, taking unnecessary risks and lacking the requisite knowledge or vigilance to recognize all risks as well the ability to naturally adjust their behaviors. However, consumers appear able to receive additional trust but if, and only if, they follow CMC's personal policy guidelines. Employees, on the other hand, are defined as potential criminals with the necessary means to commit IDT on a large scale, totally undeserving of trust. According to the business kit (2005b), they are to be closely monitored and subjected to a multitude of controls to ensure that they do not make off with the personal information of customers.

IDT, effectively, emerges as an individualized problem—a problem best dealt with at the level of the individual. It is ingrained within the market, an unforeseen consequence of data proliferation and information exchanges. As such, it is a problem that cannot be solved but only managed. The CMC documents reinforce CMC's position as a legitimate authority on the subject, able to give both consumers and businesses the tools they need to become a more trusted partner in dealing with and preventing incidences of inside jobs and IDT.

CHAPTER 5 *Data Findings and Analysis from the Royal Bank of Canada*

5.1 The Sample

This section presents the findings from employing a qualitative analysis of policy discourses found within the publicly available documents of the Royal Bank of Canada on the issue of identity theft and identity fraud. The information consists of: the client agreements (including *Client Card Agreement* and *Electronic Access Agreement*); the legal terms of use; information on RBC's privacy practices and policies[10]; and three brochures on IDT. The client agreements, legal terms of use and privacy information can be found on the Royal Bank of Canada's main website (http://www.rbc.com), through various links, and can be readily accessed by the public at large, while hard copies of the brochures are available to the public at any RBC branch.

The *Client Card Agreement* is two pages in length and sets out the terms that apply when you use your client card and your PIN, as well as your rights and duties as an RBC client (RBC, 2009a), including "your promise to be responsible for the use of your Client Card with your PIN" (*ibid*: 1).

The *Electronic Access Agreement* applies when you access or use the electronic services of RBC but does not replace any other agreement you have with an RBC Company (RBC, 2008a). The agreement totals twelve pages and includes a detailed list of key terms of use. Additionally, the document sets out the general terms and conditions for specific online banking transactions.

There are 32 text files available through the "Privacy and Security Canada" hyperlink found on the main RBC website. A list of the pages consulted is set out in References below. The files include information about user privacy, RBC's privacy policies and protections and information designed for users to protect themselves.

---

[10] This information is available through the "Privacy and Security Canada" hyperlink found on the main RBC website

There are three brochures available from RBC with information on theft including: *Personal banking and savings accounts* (totaling 22 pages) which presents detailed information on different accounts, user fees, and security features attached; *Financial Fraud* (27 pages) which outlines a number of everyday practices designed to help RBC users "prevent the theft and misuse of your personal and financial information" (2008b: 3); and *Protecting Your Privacy* (22 pages) which sets out RBC's privacy practices and information security measures.

5.2 Findings

The following section summarizes my findings of the aforementioned RBC source materials ("RBC documents"). I begin by outlining the definition of identity theft (IDT) found in the documents, and then examine five other themes found within: (1) RBC as "partner"; (2) RBC as "educator"; (3) who can and cannot be trusted in regards to IDT; and (4) the governing "rules" of banking with RBC.

5.2a RBC's Understanding of Identity Theft

RBC documents, like the CMC documents, aim to define the concept of IDT for current and potential RBC clients. According to the *Identity Theft* text file, IDT occurs "when someone steals your name… or some other personally identifying information for their use without your knowledge or consent" (RBC, 2010e: 1). Defining IDT in such manner requires the actual and necessary "use" of the information in order to be classified as such. In the *Financial Fraud* brochure (2008b), RBC further clarifies that the actual and necessary "use" of stolen information is defined solely as financial use. Financial use of the information may involve among other things, accessing and charging existing accounts, opening new accounts, writing cheques or obtaining false loans or mortgages (15). Once the information is in their possession, identity thieves may then begin to assume the identity of the victim and commit crimes in his or her name, thereby committing "identity fraud" (see also RBC, 2010e).

RBC accordingly collapses the meaning of IDT and identity fraud into a singular definition, with "identity fraud" a smaller subset of IDT. RBC's failure to specifically differentiate between the two creates additional problems. The examples RBC lists to indicate typical uses of stolen information are found verbatim in both the definition sections for identity theft (in the brochure) and identity fraud (online) characterizing IDT as a de facto financial concern—which is to be expected given that policymakers' own considerations shape the policies they create, and RBC's considerations are financial considerations (see Best, 2008 for reasoning). Collapsing the examples into a single category suggests that IDT is a problem involving clients' finances only, one that leads to monetary loss alone. This ignores broader privacy and identity concerns that accompany such incidences. The RBC definition accordingly covers both too much (including identity fraud and information misuse) and too little (financial use only, not acquisition).

While the CMC documents acknowledge that personal information may be acquired for subsequent IDT, RBC restricts the definition of IDT to instances where an assumed identity has been used with criminal intent to commit financial fraud. As such, RBC's view of the harm associated with IDT is centered around the use of the information to access financial benefits rather than the long-term consequences of having one's personal information jeopardized (e.g. feelings of increased vulnerability, loss of reputation, etc.). Constructing IDT around use means that success in dealing with incidences of IDT is defined as preventing information use and actual monetary loss.

RBC, like CMC, uses the active voice in answering the questions "What is Identity Theft?" and "What is Identity Fraud?" (RBC, 2010e: 1). On their identity theft webpage, RBC states that ID theft happens when someone steals "your name" or "your credit card number" without "your knowledge" (*ibid*), while ID fraud happens when "someone obtains another individual's personal information" and uses it to commit

financial activities in "that individual's name" (*ibid*). The differences in the chosen language may be subtle, but the effects are not. Believing that IDT is happening elsewhere, to another individual, implies "you" are protected, that ID fraud would "never happen" to you. But by placing "you" in the role of victim (i.e. "they've stolen your identity"), RBC suggests that keeping your information safe, then, is of paramount importance to you as an RBC client, and that you have a personal responsibility to find out how to better guard one's personal and financial information.

The *Financial Fraud* brochure (2008b) states that understanding IDT also means understanding "some of the methods that can be used to steal your identity" (pg. 15). The methods are important to such an understanding and are located under the heading "About Identity Theft" in the brochure as a result. The document states that such methods can range from simple theft to "rummaging through your trash or gaining access to your workplace records" (*ibid*). According to the RBC, common scams used to gain access to personal and financial data also include: "skimming"; "phishing"; "card switching" / "shoulder-surfing"; telemarketing and advance-fee scams; and current online ploys including freeware, viruses, and other malicious programs (*ibid*: 17-22; 2010b; 2010p). In highlighting areas that require closer monitoring and increased vigilance (e.g. shred your documents, lock up your workstations, install a firewall or antivirus), RBC's recommendations indicate that both past and present customer were/are at fault for not guarding these areas.[11]

RBC similarly acknowledges: "technologies can make it easier for fraud to occur" (RBC, 2010c: 1). However, where CMC made repeated mention of a risky marketplace that is larger and more complex than ever, RBC documents limit any mention to the statement above. RBC provides a number of online text files dedicated to finding out

[11] The recommendations serve as additional reasons why RBC's customer base must be investigated to ensure they did nothing that contributed to incidences of IDT.

more about the technological traps[12] that can befall unwary customers, but do not provide any context for these new problem areas. For example, RBC documents are more direct in highlighting the importance of a client's personal PIN and passwords, intrinsically technological inventions; RBC likens them to access "keys" to one's financial information and resources that must not be "revealed to anyone" but rather "kept secret at all times" (RBC, 2010h: 2; also in RBC, 2010l). Rather than revealing that RBC actually has no way of distinguishing the honest RBC customer from the identity thief if both have the "keys", RBC defines the PIN and password as crucially important pieces of information that need to be individually guarded. But nowhere do the RBC documents discuss the role that electronic identification plays in both the electronic marketplace and the growing incidence of IDT.

Instead, the RBC documents focus on the client's particular role in guarding against the crime. For example, the *Electronic Access Agreement* (2008a) warns clients that the "security of your information depends on you using safe practices" (pg. 5); this dependence means that the client, then, "*will* take all steps necessary to ensure that you do not reveal any confidential information to anyone" [Emphasis added] (*ibid*). Like the CMC documents, the RBC documents suggest that IDT is something that must be individually guarded against. But the RBC documents go further, and suggest that the individual is accountable for any instances where the individual's account is breached. Not only are costumers required to provide evidence that they took it upon themselves to learn about IDT from RBC company or another trustworthy and reputable source (such as CMC), as dictated in the *Client Agreement* (2009a). They are also required "to show on a balance of probabilities that you have not contributed to someone else's unauthorized use of your Client Card or PIN" (RBC, 2009a: 1). As a result, RBC clients

[12] Text files include: email and website fraud, protecting your computer, online privacy, securing your password, testing your computer, using a firewall, antivirus, spyware and unwanted software and proper log-offs (see References for full-list of consulted text files)

must be prepared to prove their innocence during the course of such investigations. The question then is not about how an RBC client *can* act but rather how they *must* act, and transacting business with the RBC means that one must inevitably understand and adhere to the roles and responsibilities attached in guarding against IDT.

5.2b *RBC as Partner*

Like the CMC documents, the RBC documents clearly point to a cooperative partnership required of the RBC, its clients and other organizations. The individual becomes part of this partnership by virtue of using RBC services and, in doing so, promises to be responsible for the use of agreed-upon services (RBC, 2009a). Where RBC is *understood as needing both personal information and information about their* clients needs, activities, etc., the customer is positioned as in need of RBC's expertise for the effective management of finances in the today's market economy. RBC claims that there is a wider choice of products, technologies and services granted to "you" today, and these choices "bring with them a greater need to safeguard against fraud and misuse. We can help" (RBC, 2008b: 3). Effective management is made possible through the RBC, a legitimate and trustworthy partner who is able to offer RBC clients the protection, services and peace of mind they require to bank with confidence by including guarantees, recommendations, tips and best-practice guidelines.

Working together with RBC clients is described as a best practice guideline in guarding against IDT. For example, the RBC documents suggest that: "working together is the best way"; "the best way … is for us [RBC and user] to work together" (see RBC, 2008b; 2010c). Such reciprocity is understood as a necessity in affording the best protection possible, closely linking the company, RBC, with its clientele for mutual benefit. However, not all parties are created equal within the partnership. RBC policies claim that providing information to RBC is always a consumer choice (hence the term, "volunteering" information), "but that decision to withhold may limit or prevent RBC from

providing products or services you've asked for, and makes it more difficult to advise or suggest" (RBC, 2010x: 1; see also 2010r). Taking this in mind, the customer is, nonetheless, granted a choice to limit their exposure (a key understanding in prevention according to the CMC, as already mentioned), but doing so may translate into less effective service and even prevent the original requests from being granted. Accordingly, this may be understood as not *truly* a choice at all; in essence, to maximize effect, personal information must be given and entrusted to RBC, granting them control and power over client information. This speaks to a logical flaw in the partnership rhetoric, as it underlines the lack of reciprocity and the uneven power relations between the partners, i.e. the RBC *and its customers*.

Once clients agree to a partnered approach to solve IDT, there are several rights and duties (RBC, 2009a) that they must honor and uphold. RBC believes that "while we do our utmost to safeguard your personal and financial information, we believe there are also measures you should take to help protect yourself" (RBC, 2009c: 18). In addition to sharing standard information (i.e. contact, demographic, income) with RBC, measures include: "finding out what you can do" (RBC, 2010e: 1) to avoid fraud or theft by reading the agreements and sections on RBC's websites on how to make banking more secure *regularly* and ensuring that all information provided is accurate and complete (RBC, 2008a); contacting RBC immediately if one suspects or detects unauthorized or missing transactions (RBC, 2008a; 2010h; 2010o); and, finally, complying with any obligations within the agreements or any additional instructions RBC may provide you, the user (RBC, 2008a). While a partnership is traditionally understood as cooperative, it is the individual who is to follow RBC's instructions if there is to be any partnership. These instructions intend to describe and explain the steps that the client must take to ensure the relationship between client and RBC remains intact, upheld, of mutual benefit and safeguarded from instances of IDT.

RBC's "utmost" attempts to guard against IDT include a move to partner within (amongst its own divisions, i.e. RBC investment, RBC insurance, RBC banking, etc.) and also to partner with outside agencies. These partnerships are created to comply with valid and legal information requests, to manage their risks more effectively, to meet legal or regulatory requirements (i.e. tax reporting) and to ensure the safety of its own employees, RBC clients and third-parties (RBC, 2010r). These restrictions indicate that RBC does not freely share information; besides being legally restricted from doing so (as a result of PIPEDA and other privacy legislation), RBC's own policies dictate that the company limit the number of transactions involving personal/financial information and reduce chances for thieves to intercept information in transit. This instills, within its customer base, a sense of trust in corporate practice, knowing that RBC will not jeopardize the information in making unnecessary exchanges of client information. Such a policy also reinforces unequal power relations between the client and the company—the client is to trust in and defer to the expertise of RBC and, in return, RBC will do what it can to save hapless clients from IDT.

The RBC documents espouse the importance of partnerships and how all stand to gain from them for IDT prevention; however, those partnerships are based on RBC's strict expectations of the client's behavior. And while the rules are clear, there exists a coerciveness that effectively forces the consumer into choosing between managing an successful portfolio by volunteering information and trusting in the expertise and authority of RBC and reducing the risk of data mismanagement (and IDT) altogether by withholding their own personal information and in effect choosing not to transact with the bank. Once the choice is made to entrust the information with RBC, that information is used to increase the overall number of partnerships involved, and reinforce the unequal power relations between client and company. Clients thereby agree to comply with all RBC expectations as directed or are refused access to financial services.

5.2c *RBC as Educator*

The RBC documents are positioned as educational, i.e. they communicate to the client important information that the client needs to know in order to transact business with the bank. The documents also provide answers to questions consumers may pose about what they can do to protect themselves (RBC, 2010e). The tips and recommendations are provided by way of hyperlinks featured in the *Privacy and Security Canada* (2010i) section as well as throughout the *Financial Fraud* (2008b) and *Protecting Your Privacy* (2009c) brochures.

The RBC documents reveal that effective protection is made possible in two ways: safe practices and improved knowledge. Firstly, the policy discourses found within RBC texts make numerous mentions of steps clients can take to prevent unauthorized use, noting that in addition to RBC's rigorous safeguards, there are "practices you can use" and "steps you can take to protect your privacy and identity and minimize your risks" (RBC, 2008b; 2009c; 2010e; 2010l). These different steps are provided in order to ensure that the client understands their responsibilities and acts in accordance with the needs (or wishes) of the RBC, and more broadly, the market economy. The tips to protect your identity (RBC, 2010m: 1) are listed in bulleted-form and mirror the "recommendations to combat identity theft" found within the *Financial Fraud* brochure (2008b: 16). The tips and recommendations include specific techniques such as protecting passwords, limiting access or disclosure, paying attention to financial details, and securing client information as much as possible.

RBC highlights the transitivity between one's personal / financial information and IDT, claiming that information intercept is a necessary precursor to IDT. Because the bank has no way of actually verifying the identity of those using online banking, client cards, passwords and PINs are used to identify and differentiate RBC clients. This likens clients to numbered items in the sea of RBC databases and the numbers to the

indispensible pieces of information that permit IDT to occur. One ought to ensure, then, that such information remains within the individual alone and be exchanged only with the RBC in order to guard against IDT.

In demonstrating the importance of safe consumer behavior such as signing new cards, destroying pre-approved offers and old statements, avoiding solicitations, limiting the amount of personal information carried, monitoring monthly statements, ensuring safe computer practice, and notifying creditors (RBC, 2008a; 2009a; 2009c), RBC policies reveal the information clients need to bank safely and effectively. If clients already possess the knowledge espoused from RBC policies, they are reminded, in light of the recommendations, to continue such safe practices for their own protection.

The RBC documents teach readers about the problem of IDT and strengthen the preexisting power relations between the RBC and their clients. In light of the policies, RBC clients yield to a knowledgeable source and trust that the instructions will enhance their experiences and afford them the additional protections required to guard against IDT, ensure they are doing everything they can to prevent IDT and bank with peace of mind (aided in large part to RBC's 100% online banking guarantee – see RBC, 2010h). The mental processes, which include telling clients what one ought to do and what not to do, serve to produce, reproduce and legitimate the power relations in terms of the client's own personal interests as the discourses reveal that it is their information and their finances that are at stake.

5.2d *Who Can and Cannot Be Trusted*

The RBC documents are also constructed to instill client confidence in the bank. RBC is characteristically portrayed, within its documents, as committed to its clientele and employing the tools necessary to secure, guarantee and maintain that confidence, asking clients to trust in RBC, its systems and protocol. Additionally, clients can trust that RBC is committed to customer service, protecting clients' information, and that clients,

themselves, will always have a role to play in their financial outcomes and guarding against IDT.

A particularly effective example of RBC's trustworthiness can be found in regards to one's PIN and passwords; these are presented as central to the security of the banking relationship as a whole. In numerous RBC documents (e.g. 2008a; 2008b; 2010h; 2010m), the client is expressly forbidden from ever entrusting anyone, with the exception of the RBC, with those pieces of information. The trust placed in RBC comes at the expense of social relationships—in other words, RBC is the only one whom clients can trust with their PIN, passwords, personal information and money. Clients' own spouses and children are but mere threats to the integrity and safety of one's finances. And, if for some reason, clients choose to divulge the information to family members, RBC has the right to deny reimbursement in the case of IDT, and will assume, on a balance of probabilities, that the forbidden information exchange led directly to the theft—leading them to further scrutinize and manage untrustworthy clients and their behaviors.

The online textfile on *How RBC Helps Protect You Against Fraud* (2010c) mentions RBC's built-in fraud prevention measures as part of their due diligence and constant system upgrade processes. In a sense, RBC's protective measures are understood as natural, having been built into their "normal business" practices and have led the company to employ a team of "dedicated fraud experts" working 24 / 7, while partnering closely with "industry associations, government and law enforcement" for the purposes of preventing IDT (pg. 1). With this in mind, the customer can invest and bank with confidence, knowing that a team is there, in their corner, ready to detect and respond to IDT just in case. Assurances such as these serve as evidence of the "rigorous security procedures" consumers both need and demand in today's marketplace

to guarantee that clients "enjoy doing business" in the "safe and secure environment" RBC has created (*ibid*).

RBC claims that their systems are the "most up-to-date" and meet the "highest standards" (RBC, 2010c: 1). The systems, coupled with RBC's own "internal authentication procedures", aim to ensure the highest levels of performance and satisfaction (RBC, 2008b: 10-11); they are understood to be concrete indications of RBC's commitment to client "confidentiality and security" (RBC, 2010g: 1), ensuring that prospective and existing clients are aware of the company's fluent and expansive risk management practices.

RBC offers a high level of transparency to clients, acknowledging, in the *Electronic Access Agreement* (2008a) and *Financial Fraud* brochure (2008b), the higher authorities to which it submits: the provincial legislature in which the user lives as well as federal privacy laws, i.e. PIPEDA and the Bank Act. In addition to other provisions, the privacy laws dictate that RBC "will never ask you to provide confidential information through regular mail (*ibid*: 22), and will never do so through "**unsolicited email**" [bold in original] (RBC, 2010a: 1). Additionally, RBC policy requires all employees and service providers to treat customer information in a manner consistent with both RBC expectations and with legislated privacy and security practices (RBC, 2010r), ensuring that access to customer information is restricted to only those with a "legitimate business purpose for accessing it" (pg. 1). RBC documents are clear about how they conduct their business, volunteering the information to clients under a policy of openness. In doing so, customers enjoy a high level of confidence and trust with RBC practices, knowing how RBC will conduct its business and how it will handle client's personal information behind closed-doors. This transparency is particularly useful when needed to "answer a question, solve a problem or share a success" (RBC, 2008c: 3) such as IDT and its prevention: asking what you can do to help protect against IDT, doing what is

recommended by the experts (i.e. RBC) and enjoying doing business with RBC without incident.

Some RBC practices come as a guarantee, but there are additional measures RBC *may* take as well that serve to increase consumer trust in business practice. These possibilities include: proactively contacting customers to ensure transaction legitimacy (RBC, 2010c) or to ensure your card has not been lost, stolen or used without your consent (2008b); restricting use of a Client Card, PIN or Agreement or terminating an Agreement (2009a); or declining or refusing to act on any instruction if fraudulent activity is suspected (2008a). Determining reasons about whether or not to engage in such practices appear to be based on suspicious account activity. It does not necessarily follow that RBC will employ these measures, meaning that additional harm *could* occur before RBC chooses to act, but that also means that RBC *could* prevent a great deal of additional harm if initiative is taken. According to company policy, then, RBC has the power to act in ways they see as necessary for any of the above reasons. Where the client is not given such options in all instances (say, for example, in cooperating with an RBC investigation of fraudulent activity where the penalty for noncompliance is economic and legal sanctions), RBC has the liberty to act before any report is received. Accordingly, a great number of cases never become known to clients or the authorities thereby downplaying incidences of IDT and protecting RBC's corporate image.

As noted above, RBC claims that they *may* be required to share information with others to respond to information requests, to protect employees, clients or third parties, or to help prevent fraud (RBC, 2010r). Risk management is, therefore, understood to be the driving force behind collecting and sharing information (see RBC, 2009a), and RBC claims that they will only share your information when it is in the best interest of either company or client. Clients, in light of RBC's policies and assurances, should be confident that such sharing will be done securely and safely, minimizing risk of

information misuse or mismanagement (an interesting point given the statistics on corporate data leaks above).

An underlying theme to RBC's corporate policies is their commitment to providing customers with the best possible service and to "continuously improve [their] service offerings" to customers (RBC, 2010x: 1). To do this, RBC points to specific tools ranging from collecting survey information and using persistent "cookies" or web beacons to assess online effectiveness or website functionality to providing enhanced security options allowing faster retrieval of customer information and easier log-ins (RBC, 2008a). When combined with RBC's built-in fraud prevention, these tools serve as evidence of their commitment to customers and a more effective line of RBC products or services. Once again, surveillance is justified as it both ostensibly protects the customer and enables the RBC to improve the services the customer can access.

In spite of the fine print about sharing PINs with family members, the RBC documents state that the RBC provides peace of mind in cases of no-fault IDT through their "Online Banking Security Guarantee" which will "reimburse 100% of any unauthorized transactions" to customers so long as they cooperate fully in the investigations of RBC or other public authorities (RBC, 2010h: 1; see also RBC, 2009a: 1). RBC will cover all costs where it is found that RBC was negligent in light of "reasonable commercial standards" (RBC, 2008a: 6) or for losses beyond the individual client's control (RBC, 2009a: 1). However, the insurance policy is somewhat limited, as the prevention of (and accompanying responsibility for) IDT is up to the customer—that is, to prove they did nothing to contribute to IDT. IDT is therefore Janus-faced: it can occur either through negligent consumer behavior or RBC's own negligence in not maintaining a safe environment. RBC's solution to IDT is to give clients back the money they have lost. Such policy constructs IDT as merely a financial concern, where if the money is reimbursed, then IDT harm is effectively minimized. However, in making IDT

about finances, any larger privacy or psychological concerns that accompany IDT are wholly ignored.

Like the CMC documents, the RBC documents also suggest IDT is, in large part, caused by the individual. There is a marked attempt, within the online textfiles, to ensure individuals know the steps they *can* take to prevent IDT, as well as those steps they *must* take as found in the agreements. Clients must read their agreements regularly and "must comply with any obligations" in the Electronic Agreement (2008a: 7) or the *Client Agreement* (2009a) as well as any additional instructions RBC may provide. The steps RBC identifies that one *can* take to minimize risk (RBC, 2008b; 2010e; 2010k) appear in a different light in the actual *Client Agreement* (2009a); when one agrees to use the services provided, one also agrees to all terms and conditions but also "will take all steps necessary to make sure that you do not reveal your information to anyone" (*ibid*: 1). Replacing the word "can" with "will" legally obligates the customer to comply with the required behavior as soon as they agree to use a service provided by RBC. By blurring the lines between "can" and "will", a responsible RBC client—i.e. one who takes all suggested measures without conscious recognition or sanctions and meets the needs and wishes of the RBC and marketplace—is created.

The steps RBC clients are to take to minimize their risk for IDT essentially mirror those provided earlier by the *Consumer Measures Committee* and focus essentially on: being aware of current ploys to scams and methods employed by thieves to trick naïve consumers into revealing their personal information; limiting exposure and destroying documents containing personal information; being secretive with one's information and avoiding solicitations; choosing secure and unique passwords and PINs. Should IDT happen, clients must be able to prove that they followed RBC directives in preventing IDT. Clients are made the targets of investigation, suspected of having contributed to IDT and responsible for the associated costs. If RBC's suspicions are confirmed, then it

is the consumer who will suffer the consequences, including absolute distrust from RBC and closure of account if need be.

Contributing, authorizing or consenting to an unauthorized transaction may be one thing, but RBC policies also aim to ensure that their clients are completing transactions as originally intended. Making sure that all information is accurate and complete (RBC, 2008a) includes guarding against entry errors or making transactions as a result of "mistake, error, omission, inaccuracy or inadequacy" (RBC, 2009b: 21). The fact that such a policy exists serves as evidence that RBC places more trust in the actual numbers than the client's intent. Regardless of intention, the numbers (or key entries) are understood as incapable of lying according to such policy. Since RBC is authorized to accept all electronic instruction given or "purported to be given" by the client (RBC, 2008a: 4), RBC is positioned as favoring what is tangible (i.e. numbers and entries) over the intangible (intent, error, inaccuracy, etc.).

By implying that their clients either contribute to or cause IDT, the RBC (although deserving of clients' trust) reveals its distrust of its own customer base, favoring numbers and entries over customer intent or simple human error. The investigations ensure that clients submit to the authority of RBC as the expert in all matters financial, trust and act in accordance with the rules and regulations as outlined, and internalize the "mechanisms, agents, codes and sanctions" (Gilbert, 2008: 109). By trusting in and adhering to the expert advice of the RBC, clients afford themselves additional protection against their natural tendencies to engage in risky behaviors.

5.2e *Playing by the Rules*

The standard terms and conditions of using RBC services are replete with what a client *can* and *cannot* do as well as what RBC *can* and *cannot* do in offering the services and/or products. With signing the agreement (RBC, 2008a; or 2009a), the client is legally bound to comply with all that is contained therein and must take the appropriate action(s)

as indicated. This ensures that RBC clients' behaviors are monitored and enforced, and RBC can trust that their expert instructions are being followed in accordance with the terms they have set out—if this is not the case (as found by investigation), then RBC confirms their suspicions that clients cannot by nature be trusted and must be closely regulated, legitimating their regulations as necessary components in guarding against risks. But if the rules of the game are in place, players' (i.e. clients') performances and overall outcomes can reasonably be predicted.

The agreements contain numerous mentions of their control over various products and services. In signing either a Client Card agreement or Electronic Access agreement with RBC, the client grants RBC the ability to: "add, remove, change" any parts or features of the agreement or Privacy Policy with or without notice (RBC, 2008a: 3; 2009a: 2; 2010i: 2); restrict client use of a Client Card or PIN (2009a); place "access limits" on accounts (2008a; 2009a); and add or remove entire accounts (2008a) or products and services of the RBC companies (2010f). This ensures that the RBC retains control and power over clients, adding additional instructions and stipulations as need be (to prevent IDT), restrict client use and access by claiming to do what is in everyone's best interest and add or remove services that will increase protection—i.e. if a product or service is causing additional problems or concerns with respect to IDT, RBC can remove it to minimize risk. The degree of control and trust granted to RBC by clients is substantial in the agreements.

From providing valid pieces of identification (RBC, 2009b) to upholding the responsibilities as both a cardholder (RBC, 2009a) and online customer (RBC, 2008a; 2010f; 2010h; 2010i), RBC's banking rules are provided very matter-of-factly—to do this, you must do this (e.g. to ensure your safety and an online guarantee of 100% reimbursement for fraudulent activity, you must uphold these expectations and obligations). Providing stipulations in such a manner is as part-and-parcel of the

business transaction between client and company to ensure overall banking efficiency and safety, protect all from legal liability and clarify the responsibilities, obligations and expectations attached; however, it is also an effective tool to ensure the regulation of client behavior and to quell the natural tendencies of clients to increase their risks of IDT. Deferring to the expertise of RBC and trusting that they are going above and beyond for IDT prevention purposes, clients assume the role of adherent or sidekick to RBC, trusting in their guidance and following their directives in securing a more enjoyable and safe online experience.

Once an agreement is reached and client information is submitted, RBC claims the option of either accepting or declining the information, rendering all requests subject to their standards, investigations and critique (see 2008a; 2010f). Giving information, therefore, does not necessarily mean that it will be used as intended, having to pass RBC judgment. If the submission is found suspicious or risky, then RBC will deny the request on behalf of clients, the company and its employees for the safety of all concerned. Additionally, RBC claims that their records are to be understood as "correct and binding" (RBC, 2009a: 1) and "final and conclusive" (RBC, 2008a: 8) should they ever be questioned; in claiming such, RBC effectively positions itself as more-trustworthy than clients should there ever be a conflict of records. Client recollection is understood as hazy and untrustworthy and because of this, RBC must defer to what is tangible and on-record, placing their trust in what the numbers show.

There are also particular rules contained within RBC policies that dictate what RBC is responsible for and when; RBC assumes no legal responsibility in numerous instances including: loss, damage, delay or inconvenience caused by an inability to use a Client Card; data loss including misdirected emails or text messages; and failures to access RBC agreements, instructions, information or websites (see RBC 2008a; 2009a; 2010f). Such claims chalk up these instances to technological glitches and acknowledge

that the services will not always be available to clients who must sit and wait for service to be restored. RBC claims responsibility only in cases of negligence as "determined in light of reasonable commercial standards" (RBC, 2008a: 6); typically such instances stem from "losses beyond your control" (*ibid*), i.e. where RBC, its employees or third-party service providers were responsible for unauthorized use of client information. Losses occurring because of circumstances beyond customer control can include "technical problems, RBC errors or other system malfunctions" (RBC, 2009a: 1); knowing that the system, and RBC as a whole, is imperfect and susceptible to error is especially important when understood in conjunction with the information contained within aforementioned CMC policies on the technical landscape, evolving marketplace and employee practices. The client cannot and will not have to bear the responsibility for any losses that are not within their immediate control; the rules (2009a) dictate that if clients heed the advice volunteered within the RBC documents and the specific policies, act accordingly and safely, then there is minimal, if any, responsibility attached to them in cases of IDT. As it is, IDT is characterized as an engrained and unforeseen consequence of information practice. The best way to manage IDT appears as a marked attempt to train RBC clients as responsible consumers, drawing upon various mechanisms and sanctions to ensure that they follow the trusted advice of the RBC as a partnered sidekick in preventing the crime. By using the services, the client is to have understood and agreed to all terms and instructions contained therein, legally binding them to act responsibly, never participating in, contributing to, or authorizing fraudulent activity in any manner as indicated by the rules.

CHAPTER 6

6. Discussion

Due to the complex interrelatedness of the data above, this section is designed to examine key points of interest within the documents including IDT, governance, responsibility, trust, market forces and technological advances. In this section, I discuss the main themes as found in the documents made available by both the Consumer Measures Committee and Royal Bank of Canada and situate them within the theoretical undercurrents of social construction and neoliberalism.

The documents of the RBC and CMC claim that the technological and economic landscape in which consumers find themselves has brought greater convenience to traditional tasks such as consumption, banking and communications. Within it, consumers are now provided a myriad of new technological choices (e.g. automated log-ins, accessing accounts via cellular phone) and new services (online account transfers); all of which have been proposed and embraced as self-evident solutions to social problems (Lash, 2001; Marx, 1995). Within the documents, those social problems appear human and the solutions appear technological. It is the human factor that is considered the least reliable and most unpredictable. For instance, the expanded use of PINs and chip cards has been adopted primarily to eliminate the opportunity for thieves to forge customers' signatures while PayPass has been created to eliminate the need to physically hand one's credit card over to businesses, eliminating opportunities for employees to record the card data. Businesses (RBC included) have capitalized on technology's potential and are now offering their services and products online, selling what they have always sold but in new ways and with new benefits (e.g. added controls, paying bills after-hours). Because of this, there is now something new and exciting that is being offered from the e-commerce market.

Within the CMC and RBC documents, the digital economy is defined and praised as beneficial—it grants individual consumers and clients the ability to purchase goods and services previously beyond their immediate reach, exhibit greater control over their finances and do this all at their leisure, transforming notions of both time and space. Within the e-commerce marketplace, the regular working day is prolonged. With hours earmarked for work and sleep, consumers are granted additional opportunities to shop, bank and network. It has brought about a new form of being (Dant, 2004), increased opportunities for emancipation (Habermas, 1989) and has repositioned individuals by eliminating traditional boundaries (Hayden, 2002). Although heralded as a good thing and a self-evident progression, the e-commerce marketplace has downloaded more control and more responsibility onto consumers looking to capitalize on the market's appeal, making the market simultaneously more convenient and more burdensome.

The documents define consumers as convenience-starved, requiring the option to bank or shop whenever, wherever they find the time. Bestowing upon individual users the control and rewards they seek, e-services are presented as the new norm to doing business; although faced with initial hesitancy on the part of consumers, e-services have now become commonplace and more of a necessity to daily living (D'Amico, 1998). Today, banks continually remind their clients that they can now access their accounts online, by telephone, or by mobile device—all at their convenience—characterizing a larger shift toward financial self-efficacy and governance. Consumers are understood, within the documents, as only limited by their choices—the potential is there to benefit from the market, so long as consumers place their trust in it and the institutions in power. The documents of the CMC and RBC tell clients that they will love the e-services for the added conveniences, but also reveal that those conveniences come with the downloading of individual responsibility, servile obedience to expert teaching and a consumer need to protect against new and increased risks. As such, the documents of

the CMC and RBC position the market, its overall efficiency and benefits as fundamental to their policies while promoting a neoliberal approach to online participation. Using Haggerty (2004a), the e-commerce market has converged and intensified the traditional tendencies for consumers to engage in risky behaviors due in large part to deindividuation (Hiltz et al. 1989). Accordingly, there is now an increased need to refer to the expert advice of the CMC and RBC in order to reinvent consumers (Rose, 1996a).

The technological advances employed by the RBC are routinely hailed, within the documents, as the "most up-to-date" and "of the highest standards" as can be currently (RBC, 2010c) in the market; when combined with the integrity and guarantees offered elsewhere (e.g. that CMC is working on behalf of concerned Canadian citizens), the advances are understood as vehicles in which consumer trust can and should be placed. The documents replace the traditional relations of trust—i.e. family, friends—with technological trust for the instrumental purpose of having consumers trust in the market and its processes, equating it strongly with progress. The productive forces of RBC's policy discourses in the documents and the specific wording of the language (e.g. "100%" banking guarantee) is indicative of their orientation in having consumers participate and increasing social effectiveness of their banking practices. This social effectiveness within the documents establishes and cultivates customer belief and trust in the legitimacy of the market and RBC's own hegemony vis-à-vis other Canadian banking institutions in guarding against IDT. The RBC is defined as committed to the issue and able to handle the risks of IDT through the various mechanisms at their disposal—of which, the client is the characterized as the most effective line of defense. CMC's documents are also directed to establish and foster such belief and trust in the market, and highlight their operations to "improve protection for consumers on several fronts" (CMC, 1998: 1). Applying Fairclough and Wodak (1997), the policies of the CMC and the RBC are fluent and expansive in the following ways: they work on behalf of all

consumers and clients to create more effective products and services; facilitate and call for increased regulations and protections; foster and promote initiatives such as fraud-prevention month and information-sharing; and finally, work through individuals, their fears and wants to transform them into more effective consumers and establish a "disciplinary society" (Foucault, 1979). The documents claim that the CMC and RBC will protect agreeable consumers and, at the same time, improve the services provided—justifying the surveillance of consumers and increasing the visibility of behaviors.

The freedoms individuals enjoy within the marketplace are not necessarily free. As Rajchman (1991) and Gordon (1991) previously found, individuals have been economically willing to do their bit in maintaining the systems that define and delimit them, and play their parts in a market game whose intelligibility and limits they take for granted. By agreeing to participate in the market, abiding by the conditions outlined specifically with RBC, and trusting in the expert advice of the CMC and RBC, free individuals are enjoined to govern themselves and their finances, promote and secure their own well-being, capital and liberty characteristic of the neoliberal agenda. The policy discourses found within the documents of CMC and RBC rule individuals through the freedoms and choices offered rather than despite them. They align individuals' motivations (i.e. increasing capital) with CMC's and RBC's own political and economic objectives (i.e. trust and embrace the market and become a normalized, participating consumer) and turn consumers into allies in the continuous fight against IDT, promoting an end that was no part of the original intention.

Having grown exponentially, the e-commerce marketplace necessarily requires a more sophisticated and knowledgeable user to navigate effectively and safely. RBC and CMC act as guides that will show individuals how the market is to be navigated by way of recommendations, tips, guidelines and warnings—legitimizing their presence in doing so. For consumers, there is, after all, little to no choice to participate and there is no such

thing as partial participation. It follows that volunteering personal information is a necessary component if there is to be any hope for consumers to secure mortgages, credit or loans, rent movies, purchase warranties and so forth. While the reality is that people must participate, *effective* participation becomes a moral teaching according to the documents; consumers *have* to protect themselves, stabilize any effect of their personal and conjectural information (Latour, 1991), promote and secure their capital according to the information, but are also made to believe that this is what should be done. IDT is, therefore, not only a matter of conveniences and inconveniences but also of morals—it is right and good to self-manage.

The services and lure of the market are motivating factors for consumers, but, by agreeing to use the services and participate in the market, consumers simultaneously increase their risk of IDT. Such risk is manageable, and consumers should accept the risk (and their lot-in-life) because there are things they can do to prevent IDT and there is also something better that will come with participating. Towards this end, the power structures have been formalized and institutionalized, fixed by both customs and regulations of the CMC and RBC, to encourage individuals to behave in accordance with the needs of the market and to self-identify with others as responsible consumers making responsible choices.

While the market and the services are praised as all glitz and glamour, there is, at the same time, something bad which consumers are made aware of. IDT is, according to the documents, endemic to technology (see CMC, 2005d; RBC, 2010c). CMC and RBC present IDT as a "worsening situation" (Best, 2008: 33-35) that is closely tied with technological and economic advances; as evidence, CMC claims there has been a 500 percent increase in reported cases of IDT from 1999 to 2002 alone (CMC, 2005d: 6). Since "a big number suggests a big problem" (Best, 2008: 33), those who hear such a claim will, then, have a personal and valid interest in ensuring they remain unaffected by

the epidemic of IDT. RBC agrees that progress has made fraud easier to occur, but does not acknowledge the frequency at which they are affected by data breach or IDT and for good reason; there is a deep-rooted interest for RBC to keep the information under-wraps—to prevent such incidences from reflecting poorly on the company in the long term (CMC, 2005b: 14). RBC obfuscates their own numbers on IDT, incorporating it into their "normal business" practices (RBC, 2010c: 1), to make consumers believe in the legitimacy of the market while keeping them apprised of an amorphous risk and an accompanying moral need to be responsible. RBC, therefore, characterizes IDT so as to forego any negative stigma that may accompany evidence of their susceptibility and increase their own worth to Canadians.

Thieves have exploited the same tools (i.e. information databases, payment systems) businesses employ and the entire economic landscape to their full criminal potential leaving governments, businesses and law enforcement trying to fix a social problem that may not be entirely fixable. The studies of Perrow (1984) and Schreft (2007) have confirmed that information technologies increase the likelihood of system failure, misuse of information or data breach and make organizations more difficult to manage—this appears valid within the sample; according to the CMC (2005d), market practices themselves have made the situation worse with more and more consumers relying on credit to make purchases and making those purchases unsecured. Despite the best efforts of government to tighten the market, previously-lax business regulations and current IT/market practices have led IDT to be viewed, within the documents, as but an inevitable consequence of progress, illustrating a social reality that would have otherwise remained masked—that the systems themselves, as known targets of identity thieves and recognized choke-points of commerce funneling high volumes of clients and information through one service (Rigakos & Hadden, 2001), is cause to IDT. CMC and RBC claim that with risk comes reward—the market holds the answers consumers seek

to complex financial matters, and the information provided by the CMC and RBC will ensure that any risks for IDT are kept to a minimum. Since the CMC and RBC cannot afford to have consumers opting out of the marketplace—for fear of upsetting the entire economic system—IDT must be, and has been, defined in a particular manner.

The definition of IDT, used by both the CMC and RBC, stays within a neoliberal frame. According to the sample, IDT focuses on harm to an individual victim ("you") by an individual offender. While it could mean that CMC and RBC are blind to systemic causes of IDT, this is not the case since both acknowledge that technologies and progress has made IDT easier for thieves to commit; in effect, both the CMC and RBC are working a double-game. The systemic problem of IDT is not seen as the security or information loopholes that will harm individuals—since the harm can be minimized if individuals view IDT as a personal concern and take appropriate preemptive action—but rather the possibility that individuals will recognize the potential harms and opt out of the e-commerce model altogether. To guard against this, the CMC and RBC have defined IDT as an individualized problem, and focus on specific things that the individual consumer can do to prevent IDT and how they can respond effectively should IDT happen anyways.

For our purposes, this specific type of power is better understood as disciplinary control, and it is through such control that the CMC and RBC reveal their exercises in power *through* individual consumers, asking them (and later obliging them) to align their own wants and motivations with others as part of a larger flock (Foucault, 1979) led by an invisible hand to a more efficient economic model. The definition of IDT employed by CMC and RBC deflects criticism away from a fundamentally flawed economic system, teeming with risks, and makes individuals (and employees) feel responsible for the IDT problem. Once individuals agree to use the system, they agree to accept the accompanying risks and mechanisms of governance. Unfortunately, the documents of

the CMC and RBC claim that the individual is the primary risk. While it has always been expected that individuals govern themselves responsibly (O'Malley, 2008, Foucault, 1979), there is no guarantee. Individuals cannot be trusted to do so, their behaviors cannot be taken as a given and they must be monitored. Foucault (1982) claimed that there are several kinds of conduct, several possibilities for behavior in every situation, and the goal for CMC and RBC then becomes one of securing a particular kind of conduct and a specific way of reacting to the social problem of IDT. By agreeing to participate, individuals essentially agree that they are the risk that needs to be managed, that they are *bad* and in need of expert and moral instruction, while the CMC and RBC are *good*—i.e. consumers' saving grace and guides. In accepting the neoliberal responsibility to self-govern, they are drawn into the market game as the key player and partner; but at the same time, doing so has implicated the consumer as the one deserving of blame when it comes to IDT.

While the system has made it easier for thieves to steal personal information, IDT is presented as 'nothing you cannot handle' and a risk that is not worth taking. The documents of both the CMC and RBC claim that there is a way to navigate the e-commerce system that will minimize IDT risk. This effectively constructs IDT as a social problem that is to be solved (insofar as it can be solved) at the level of the individual. Using Wall (2001), it is the e-commerce model that has challenged the conventional understanding of IDT and effective policing—it has transformed a systemic flaw into an individualized concern and has made the consumer the most effective mechanism to deal with IDT. Within the documents, it is the individual that is defined as a manageable product and the 'binding glue', of sorts, that will fill the holes left by the system. They are characterized as being amenable to expert instruction and instilled with a sense of personal obligation to guard against IDT ("you will take all steps necessary"—see RBC, 2009a: 1) and remain accountable for their actions and inactions ("security of your

information depends on you"—see RBC, 2008a: 5). In agency-specific terms, individuals need to be made into better consumers or employees: prudent, rational and responsible by way of trusted and expert advice, subject to increased surveillance of their risky behavior and disciplinary control (Garland, 2001; Wacquant, 2001; Haggerty, 2004a).

Within the documents, individuals are defined to be natural risk-takers, mistake-prone and a danger to themselves: carrying too much information, not locking up personal information, not shredding bank statements, not speaking discreetly, etc. A responsible person should naturally refrain from volunteering account numbers and passwords to passersby, but the CMC and RBC find it necessary to remind clients to guard against such simple errors, indicating a level of condescension on par with being reminded to 'look both ways before crossing the street.' Within the documents, individuals fail to possess an acute awareness of their self and their data-doubles (similar to the findings of Postmes et al., 1998) and exhibit a reduced ability to engage in long-term rational planning (found previously in Zimbardo, 1969) when it comes to taking IDT precautions such as reducing exposure, choosing alpha-numeric passwords and so forth. The documents claim that there is an acceptable level of exposure that comes with participating in the market economy, but at the same time, consumers' natural tendencies have exposed themselves to dangerous levels. Their risk knowledge is understood to be lacking; knowing that their knowledge of IDT is limited and will not self-actuate into the appropriate behaviors, the CMC and RBC appear as experts upon whom consumers are to rely on for the expert information and guidance needed. Applying Burchell (1991), individuals, being the subject of particular market interests, have become the correlate and instrument of a new form of government—a neoliberal form of government—that entices the population to evaluate itself as a risk and conduct itself in accordance with the CMC and RBC.

In addition to the encoded norms of society (e.g. do not share your account information or passwords with others), the documents highlight the preventive practices consumers can undertake in order to curb their risky tendencies and readily provide readers with "what to do" sections. As noted, "the self is to style its life through acts of choice, and when it cannot conduct its life [accordingly], it is to seek expert assistance" (Rose, 1996a: 158). Clients, defined in a position of need, are told the truth about IDT (what it is, what is considered safe/unsafe, what you can do, what to guard against) and are empowered within the documents to police themselves in accordance with the expert knowledge of the CMC and RBC, which exhibits strong characteristics of broader, neoliberal forms of governance.

The documents present particular knowledge-claims and illustrate true examples of consumer faults, employee insiders and criminal methods which they have been made aware of, either through their own investigations or outside information. The documents' understanding of IDT ultimately shifts accountability for IDT onto individual consumers/clients; the information is presented with moral and civic undertones so that they may internalize the knowledge and adjust their naturally risky behaviors accordingly to secure better protection in market transactions and avoid costly incidences of IDT paralleling Foucault's (1991a) "technologies of the self." The information permits individuals by their own means and with the help of others (the institutions) to produce a certain number of operations, rational thoughts and responsible behaviors for purposes of transformation. The documents of the CMC and RBC present IDT as an amorphous and continual risk to consumers—thieves will peer over shoulders, install viruses on computers, rummage through garbage, intercept wireless communications, etc.—to ensure that the consumer maintain that constant eye for improvement, be on-guard at all times, dissect their behaviors and evaluate all potential threats. The documents compel the consumer to decipher themselves in relation to what is forbidden—or cause to IDT—

and recognize those areas of their life that need work. CMC and RBC remind individuals that thieves are always watching and waiting for the opportunity to steal the information in hopes that consumers will take all recommended steps to quash the potential for harm. The attempts made are indicative of the key components of panopticism as detailed by Foucault (1979): that the surveillance be permanent in its effects (even if discontinuous) and render the actual exercise of power unnecessary as the consumer now becomes the principle of their own subjection, governed through that which they value. As such, the individual consumer's rights are redefined, by the documents, as manipulable consumer choices.

In the process of claimsmaking, CMC has also listed typifying examples of what may happen to victims to IDT in support of responsible consumer action. The examples of what can happen to victims are, in fact, "rarely typical" according to Best (2008: 32) but are chosen rather to illustrate the seriousness of the problem to order to build rhetoric and persuade readers why they should act in accordance with CMC's and RBC's instructions. So, in making the claim that victims may spend "hours trying to clear their names", "suffer emotional anguish" and "loss of reputation" making it "difficult for victims to find employment or get access to credit when they need it" (CMC, 2005d: 7), CMC has advantageously used the effects as "warrants", explaining to potential victims why something should be done about IDT preemptively. The specific remedy to the problem of IDT is the neoliberal idea of "caring for the self" (Rose, 1996a), a concept of individual governance, beckoning individuals to continue making risk assessments of potential harms during the continual "business of living." Using Lash (2001) and Marx (1995), this is the self-evident solution to IDT proposed within the documents of the CMC and RBC—IDT is caused by the individual, and any remedy, if it is to be successful, must then begin and end with the individual.

There will be some consumers who, as a result of hearing the recommendations and warnings, alter their naturally risky behaviors; to apply Garland (2001), there are norms for consumers to follow, but there is no guarantee that consumers will follow the information and change their behaviors. To secure the guarantee of responsible behaviors, the steps one "can" take become steps one "must" take and the recommendations become rules that are to be followed—which is exactly what happens when agreeing to bank with RBC. In giving their information to reputable organizations such as RBC, consumers enjoy additional protections and improved service but also agree to abide by the terms and conditions attached, take all measures RBC sees as necessary (recognized by the CMC as the best-practices) to guard against IDT, and open themselves to investigation. Although the steps and tips provided by CMC and RBC are provided as the authoritative norms to manage one's risk, they are transformed into *legal* and *financial* obligations to act responsibly within the terms and conditions so as to meet the basic needs of the "economic man" (Burchell, 1991) and solve the problem of IDT.

The documents and constructions, therein, claim that, on their own, consumers/clients cannot be trusted to act responsibly; accordingly, there are rules in place to ensure the automatic functioning of power, coordination of will and the "conduct of conduct" (Rose, 1996a). If the individual does not want to be held responsible for unauthorized transactions, they must act in accordance with the instructions provided, following the wishes of the RBC (which are one and the same as the wishes of the CMC). Mobilizing Best (2008), the claims within the documents define IDT in a manner to persuade readers that there is something wrong with them needing to be solved. In agreeing to the terms and conditions, the legal and economic sanctions (being an accessory to IDT) are then imposed, internalized and activated involuntarily by the reinvented client to guard against any such possibility.

The documents define IDT as a personal (yet collective, since it affects all) cause for concern, deeply involving the individual in the matter and increasing the likelihood that they will make informed and appropriate decisions about their online safety practices (see Larose et al., 2008). The client is made the subject of investigation—to confirm that they did everything in their power to prevent the unauthorized use of their personal information for IDT purposes—and the target of the RBC, inducing within the client the "conscious and permanent visibility" that guarantees their responsible behavior (Foucault, 1979: 201). RBC records, understood as "correct and binding" on clients (RBC, 2009a: 1), are called upon as evidence of their client base's accountability and untrustworthiness; each customer is to have their own documented evidence to support their innocence, pitting them against the authority of the RBC. The hegemonic rights and privileges constructed within the policies of RBC lead to a greater understanding of how the "mega-discourse" (Alvesson & Karreman, 2000b) of power shapes the social, legal and economic realities of banking with RBC, reinforces the (veiled) power relations, and constrains the clients as subjects therein. By making IDT a personal issue (something that individuals must guard against and prove they had no part of), the RBC conducts and ensures the responsible behavior of individuals for their own safety but also in keeping with the larger wants, needs and expectations of the CMC and the market economy—characteristic of the neoliberal model and Foucault's (1991a) "technologies of the self."

The language employed by CMC and RBC within the documents characterizes reciprocity as a critical component to guard effectively against IDT. Working together is seen as the optimal way to deal with IDT, but in actual fact, it is the consumer who is defined as risky, needing to do what they are told. Even though the system is bound to cause grief to many individuals, the CMC and the RBC position the market and themselves as trustworthy and their information as reliable and true. By necessarily

sharing personal information and agreeing to participate in the new economic model, the individual and bank form a mutual degree of trust—both the CMC and RBC appear as legitimate authorities on the subject of IDT, able to offer consumers the oversight, solutions and skills they need to navigate the market without incidence and benefit fully in the digital economy (Industry Canada, 2009a). Similar to the findings of Caeton (2007), for individuals to escape the insidious threat of IDT, they willingly enter the protective custody of RBC and CMC and accept the oversight of their behavior, trusting them to store and protect the data that have come to represent their identities (Haggerty & Ericson, 2000), while individuals agree to care for themselves more effectively in the style of Rose (1996a). This strongly reinforces the uneven power relations that exist between the institutions and consumers. Specifically, the institutions of CMC and RBC have promoted rationalized and technological policies within the documents to steer the actions of consumers and clients (deemed the 'targets of government' – see Foucault, 1991) in pursuit of certain neoliberal ends (Rose, 1996a; Miller & Rose, 1990; Miller & Rose, 1992). When the protections fail, it is the businesses that are defined as the consumers' saving-grace—able to reimburse monetary losses in cases of no-fault IDT, even though they, themselves, have set up the very foundation that grants thieves the increased opportunities to commit IDT in the first place.

The overall outcome, in providing the information on what may happen when IDT happens, appears to be the granting of knowledge to the individual user so that they may become empowered, more aware of and accountable for their actions, taking all precautions outlined within the CMC and RBC documents. Given the claims made about what should be done to combat the problem of IDT, it is realistic to see that individual consumers and clients will begin to act as self-interested agents, basing their financial decisions vis-à-vis banking and IDT risk on rational, prudent and supposedly "free choice" (characteristic of the public-choice model – see Rose, 1993). But in order to

benefit fully from the marketplace, the consumer must volunteer their personal information and place their trust in the processes—meaning that the neoliberal demands imposed on individuals are at odds with the restructuring of their economic-being in the market economy. In making this higher risk-higher reward decision, consumers simultaneously increase their own risk of IDT and rely on expert knowledge to minimize that risk. Consumers, in reading the documents, understand the risks involved, and the choice to continue participating is made freely; they trust that the market holds the answers they seek to complex problems and the expert advice of the CMC and RBC allows for a productive, prosperous, enterprising, and fulfilled banking experience. Simply put, "we have tied ourselves 'voluntarily' to the knowledges that experts profess, and to their promises to assist us in the personal quests for happiness that we 'freely' undertake'" (Rose, 1996a: 77). The policy discourses presented in the documents of RBC (2010f) indicate the constraining effects that have been placed on its customers, shaping the social reality (that information should be volunteered) and instigating customer action in the process. This has the effect of strengthening already unequal power relations with the partnership as consumers have embraced the neoliberal model and have chosen to buy-into the market process, yielding to the authorities of both the CMC and RBC.

IDT is presented as a problem that cannot be eliminated, characterized as the 'way things are'; the documents of the CMC and RBC, and the policy discourses found therein, aim to manage the social problem of IDT by affecting positive change and informed consumer action in the limitless, "borderless" and risky marketplace, amounting to both problem and risk management. It appears as though individuals have been quick to accept notions of online self-efficacy, *but* lack the tools and information to effectively regulate their natural behaviors. With the requisite knowledge, individuals are made into professionals, of marginal-utility to altogether preventing IDT—since it will more than

likely occur by way of corporate data breach according to statistics—but of maximal benefit to the overall health of the economic system as a participating, informed and responsible consumer.

The solutions contained within the policies represent excellent examples of broad forms of neoliberal governance with a marked shift away from state-owned responsibility. The discourses of both the CMC and RBC highlight the necessity for individual self-governance and self-responsibilization and present the documents in hopes of changing previously risky consumer behaviors in face of new, expert knowledge. CMC and RBC are both presented as facilitators, smoothing consumers' transition from risky to responsible behaviors while offering additional protections through tightened regulations or improved protections (e.g. information-sharing networks, banking guarantees).

And by highlighting the governing "rules", within the agreements, terms and conditions of use, the documents claim to define exactly what is and what is not responsible consumer action, and ensure responsible behavior through said definitions, typifying examples, figures and legal limits—effectively governing the individual from-a-distance and monitoring their actions. The rules are interpreted as mechanisms of governance employed by the RBC that produce and sustain the elements of truth (what is accepted procedure) and aim to ensure consumers do nothing to contribute to IDT. The most direct solution to IDT appears as an attempt to educate individual actors with the hope that they, as a result of proper guidance and instruction, will be able to differentiate what is safe from what is unsafe, and it is with such purpose that the policies of the RBC and CMC seem to organize themselves. Taking and internalizing these rules, the consumer, and business for that matter, will be in a position better-equipped to manage online risks, yet effectively constrained within the market game,

subjected to the multiplicity of legal mechanisms and sanctions that may be enacted should they fail to live up to reasonable expectations.

Specifically, the end result is a more responsible population of market players, acting not only in their own best interest but also in the overall interests of the entire market and its group of partners, saving all involved valuable time and resources in combating IDT. The policy discourses contained within the documents may be understood as legitimate and well-intended; they represent real concerns that consumers and businesses *must* be made aware of; however, the effects of the discourses reach levels that may or may not have been intended including the construction of IDT as an individual, rather than corporate, problem and passively coerce individuals and employees into making healthier choices in keeping with the wants and needs of larger economic and political forces characteristic of the neoliberal model.

CHAPTER 7

Conclusion

The information presented relies heavily upon the interrelationship between power, disciplinary control and discourse, and creates strong meanings and effects for individual consumers within the neoliberal framework. This study examined the policy discourses presented within the publicly-available materials from both the *Consumer Measures Committee* and the *Royal Bank of Canada* on the issue of IDT and its direct effect on subjects—why IDT is defined the way it is, what do their policies say about the causes of IDT, what are the risks of IDT and are they manageable, and if so, how. In doing so, the study has revealed the productive and constitutive powers of discourses veiled within the documents, establishing and revealing how the claims are founded and how the constructions are operationalized, practiced and supported amongst the myriad of partners involved in IDT prevention efforts. By revealing the subversive meanings and interpretations of policymakers' conceptualization of IDT, this study has described and explained how individuals and their natural tendencies bring unparalleled risks to the market economy. Within the documents, individuals have been defined as e-subjects of the CMC, RBC and the market itself. This finding is strongly in keeping with existing studies in governmentality. The social construction of IDT has implicated individuals as subjects of multiple forms of covert governance. Those mechanisms have worked through individuals, their fears and their beliefs in securing a more prosperous market experience. This thesis has found that previous academic work in social constructionism (e.g. Best) and governmentality (e.g. Rose) serve to complement each other and work hand-in-hand in the following ways.

The policy discourses in the documents erroneously perpetuate the *social* problem of IDT as an *individualized* problem—committed by individuals against other individuals—rather than from the corporate and government bureaucracies that promote

the quantifiability of identity in the information marketplace. This study also found that the bureaucracies of the CMC and RBC attempt to foster trust in the market, in spite of the fact that it is bound to cause consumers grief. The risks of IDT are presented as manageable, and worth taking, so long as consumers follow the advice of the CMC and RBC, trusting in their practices while, at the same time, agreeing to become more responsible consumers in accordance with the needs of the e-commerce market and of neoliberal aims. The proposed solutions have included: caring for the self; increased disciplinary control and surveillance of risky populations and behaviors; and rational and prudent economic choices—all of which are found and promoted within the new "art of government" that is neoliberalism (Burchell, 1991). This study has identified the CMC and RBC as expert facilitators and trustworthy partners who claim to be able to grant consumers and clients the tools, reliable information and guidance they need to protect themselves in a borderless marketplace. IDT has been presented so as to rearrange the power dynamics, diverting blame away from the bureaucratic models while promoting a spurious, individualized solution to a growing social problem.

Ultimately, this research project has highlighted the various claims being made about IDT, understanding both the specific constructions of IDT mobilized by the CMC and RBC and the solutions they recommend. This thesis has deconstructed the underlying assumptions of the claims shared by both the CMC and RBC so that individuals, consumers and clients may have the ability to see behind the policy language, change their own perceptions of a growing social problem and institute new forms of mutual-dialogue and debate between the governing and governed in devising effective solutions.

Future research needs include more detailed and better quality data on exposure effects to the mechanisms of IDT governance using focused interviews and surveys that capture the full distribution of emancipatory education efforts on IDT. Important

examples include detailed data on responsible behavior patterns, individual markers for accepting and internalizing recommended and instructed behaviors, and better indicators for individual consumer sentiment, namely: having been identified as such, do people actually feel responsible for the IDT problem? Do they follow some or all of the recommendations? Do they feel their efforts make a difference? This particular research study concerned itself with exposing the policies and the underlying meanings rather than attempting to directly quantify these and other effects of the policies.

This is a substantial research agenda, and one for which some progress has been made within this study. This study has detailed the social construction of IDT and examined the solutions contained within the documents from a governmentality perspective. Public policy needs dictate that greater priority is given to research that more reliably and relevantly identifies the potential effects of the claims being espoused within various documents in regards to IDT. Such research will undoubtedly provide a more compelling basis for massive increases in preventive efforts that is to be required if IDT is to be a problem capable of being solved.

REFERENCES

Aas, K.F. (2007). Beyond 'The Desert of The Real': Crime Control in a Virtual(ised) Reality. In Y. Jewkes (ed.), *Crime Online*. Cullompton: Willan Publishing.

Agger, B. (1992). 'The discourse of domination' , in *The Frankfurt School to Postmodernism*. Evanston, IL: Northwestern University Press.

Alvesson, M. & Deetz, S. (1996). Critical theory and postmodern approaches in organizational studies. In S.R. Clegg, C. hardy, & W.R. Nord (eds.). *Handbook of organization studies (pp. 191-217)*. London: Sage.

Alvesson, M. & Karreman, D. (2000b). Varieties of discourse: On the study of organizations through discourse analysis. *Human Relations*, Vol. 53: 1125-1149.

Anderson, K.B, Durbin, E. & Salinger, M.A. (2008). Identity Theft. *Journal of Economic Perspectives*, Vol. 22 (2): 171-192.

Anderson-Gough, F., Grey, C., & Robson, K. (2000). In the name of the client: The service ethic in two professional services firms. *Human Relations*, 53, 1151-1174.

Babbie, E. (2004). *The Practice of Social Research* (10th Ed.). Belmont, CA: Thomson Wadsworth.

Bargh, J. A. (1988). Automatic information processing: Implications for communication and affect. In L. Donohew, H. E. Sypher, & E. T. Higgins (eds.), *Communication, social cognition, and affect* (pp. 9–32). Hillsdale, NJ: Lawrence Erlbaum Associates, Inc.

Bargh, J.A., McKenna, K.Y.A. & Fitzsimons, G.M. (2002). Can You See the Real Me? Activation and Expression of the 'True Self' on the Internet. *Journal of Social Issues*, Vol. 58(1): 33-48.

Barney, D. (2004). *The Network Society*. Cambridge: Polity Press.

Barry, A. et al. (1996). *Foucault and Political Reason*. London: UCL Press.

Barrett, N. (1997). *Digital Crime: Policing the Cybernation*. London: Kogan Page.

Bauer, K. & Hein, S.E. (2006). The effect of heterogeneous risk on the early adoption of Internet banking technologies. *Journal of Banking & Finance*, Vol. 30: 1713-1725.

Bauman, Z. (1992). Intimations of Postmodernity, London: Routledge.

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

Becker, H.S. (1967). Whose Side Are We On? In Carroll, W.K. (ed.), *Critical Strategies for Social Research* (pp. 23-29). Toronto: Canadian Scholar's Press Inc.

Bell, D. (1973). *The coming of post-industrial society: A venture in social forecasting*. New York: Basic Books.

Bell, D. (2007). *Cyberculture Theorists: Manuel Castells and Donna Haraway*. London: Routledge Publishers.

Bell, V. (1993). *Interrogating Incest: Feminism, Foucault and the Law*. London: Routledge.

Benson, M. (2009). Offenders or opportunities: Approaches to controlling identity theft. *Criminology & Public Policy*, Vol. 8 (2): 231-236.

Berg, L. (2004). *Qualitative Research Methods for the Social Sciences* (5th ed.). Boston, Pearson Publishing.

Berger, P.L. & Luckmann, T. (1966). *The social construction of reality: A treatise on the sociology of knowledge*. Garden City, NY: Anchor.

Best, J. (1990). *Threatened Children: Rhetoric and concern about child-victims*. Chicago: University of Chicago Press.

Best, J. (2008). *Social Problems.* New York: W.W. Norton & Company.

Bernstein, B. (1990). *The Structuring of Pedagogic Discourse*. London: Routledge.

Bloor, M. & T. Bloor (2007). *The Practice of Critical Discourse Analysis: An Introduction*. London: Hodder.

Bocij, P. (2006). *The Dark Side of the Internet: Protecting Yourself and Your Family from Online Criminals*. Westport: Praeger Publishers.

Bouckaert, J. & Degryse, H. (1995). Phonebanking. *European Economic Review*, Vol. 39: 229–244.

Bourdieu, P. (1998). The Essence of Neoliberalism. *Le Monde Diplomatique*, December. Available at: http://mondediplo.com/1998/12/08bourdieu

Branigan, S. (2005). *High-Tech Crimes Revealed: Cyberwar Stories from the Digital Front*. Boston: Addison-Wesley Publishers.

Braithwaite, J. (2000). The New Regulatory State and the Transformation of Criminology. In D. Garland and R. Sparks (eds.), *Criminology and Social Theory*. Oxford: Clarendon Press.

Brock, D. (2003). Moving Beyond Deviance: Power, Regulation and Governmentality. In D. Brock (ed.), *Making Normal: Social Regulation in Canada*. Scarborough: Nelson Thompson Learning.

Brown, S. (2006). The criminology of hybrids: Rethinking crime and law in technosocial networks. *Theoretical Criminology*, Vol. 10(2): 223-244.

Bryman, A. (1988). *Quantity and Quality in Social Research*. London: Unwin Hyman.

Burchell, G. (1991). Peculiar interests: civil society and governing 'the system of natural

liberty.' In G. Burchell, C. Gordon and P. Miller (eds), *The Foucault Effect: Studies in Governmentality*. London: Harvester Wheatsheaf: pp. 119-150.

Burr, V. (1995). *An Introduction to Social Constructionism*. London: Routledge.

Burrows , R. & Loader, I. (1994). *Towards a Post-Fordist Welfare State?*. London: Routledge.

CALPIRG and Privacy Rights Clearinghouse. (2000). Nowhere to Turn: Victims Speak out on Identify Theft. See also General Accounting Office (2002). GAO-02-363.

Cabinet Office (U.K.). (2002). *Identity Fraud: A Study*. London: Economic and Domestic Secretariat, Cabinet Office.

Caeton, D.A. (2007). The Cultural Phenomenon of Identity Theft and the Domestication of the World Wide Web. *Bulletin of Science Technology & Society*, Vol. 27(1): 11-23.

Canada. Parliament. House of Commons. An Act to amend the Criminal Code (identity theft and related misconduct). Bill S-4. 39th Parliament, 1st Session, 2009-2010. Ottawa: Public Works and Government Services Canada – Publishing, 2009. (Revised 5 June 2009).

Canadian Association of Police Boards. (2008). A Report on Cybercrime in Canada.

Canadian Intergovernmental Conference Secretariat. (2004). Backgrounder: Consumer Ministers' Meeting. Winnipeg. Retrieved February 12, 2009 from World Wide Web: http://www.scics.gc.ca/cinfo04/830807005_e.html

Capeller, W. (2001). Not Such a Neat Net: Some Comments on Virtual Criminality. *Social and Legal Studies*, Vol. 10(2): 229–42.

Chodos, R., E. Hamovitch, & R. Murphy. (1997). *Lost in Cyberspace? Canada and the Information Revolution*. Toronto: James Lorimer & Company Publishers.

Chomsky, N. (2003). *Profit Over People: Neoliberalism and Global Order*. New York: Seven Stories Press.

Chouliaraki, L. & Fairclough, N. (1999). *Discourse in Late Modernity: Rethinking Critical Discourse Analysis*. Edinburgh: Edinburgh University Press.

Chua, J. (2003). Identity theft: Robbery in the new millennium. *CBC News*. Available at: http://www.cbc.ca/consumers/indepth/identity/ (accessed November 7, 2006). Cited from Winterdyk and Dyk (2008).

Cicciretti, R., Hasan, I. & Zazzara, C. (2009). Do Internet Activities Add Value? Evidence from the Traditional Banks. *Journal of Financial Services Research*, Vol. 35: 81-98.

CIPPIC (2007a). *Canadian Legislation Relevant to Identity Theft: Annotated Review*. CIPPIC Working Paper No.3A (ID Theft Series). March 2007. Ottawa: Canadian Internet Policy and Public Interest Clinic.

CIPPIC (2007b). *Enforcement of Identity Theft Laws*, CIPPIC Working Paper No.5 (ID Theft Series). July 2007. Ottawa: Canadian Internet Policy and Public Interest Clinic.

Clark, R.V. (1995). "Situational Crime Prevention." *Crime and Justice* 19, 91-150.

Clark, B. (1998). *Political Economy: A Comparative Approach* (2nd ed.). Westport: Praeger Publishing.

Clarke, R.V. (2001). *Shoplifting*. Problem Oriented Guides for Police No. 11. Washington. DC: Department of Justice, COPS, and Center for Problem Oriented Policing. Available at: http://www.popcenter.org/Problems/problem-shoplifting.htm.

Clegg, S.R. (1987). The language of power and the power of language. *Organization Studies,* Vol. 8, 61-70.

Coleman, W.D. & Porter, T. (1996). Banking and Securities Policy. In Doern, G.B., Pal, L. & Tomlin, B.W. (eds.). *Border Crossings: The Internationalization of Canadian Public Policy.* Toronto: Oxford University Press (pp. 55-81).

Collins, J.M. & S.K. Hoffman. (2004). *Identity Theft Victims' Assistance Guide: The Process of Healing*. New York: Looseleaf Law.

Comaroff, J. & Comaroff, J.L. (2000) Millennial Capitalism: First Thoughts on a Second Coming. *Public Culture*, Vol. 12(2): 291–343.

Consumer Measures Committee (1998). *Consumer Ministers Take Action on Consumer Fraud* [Online textfile]. Ottawa: Consumer Measures Committee. Retrieved December 10, 2008 from World Wide Web: http://www.cmcweb.ca/idtheft

Consumer Measures Committee (2001). *Consumer Ministers Take Action to Improve Consumer Protection in the Evolving Marketplace.* [Online textfile]. Ottawa: Consumer Measures Committee. Retrieved December 10, 2008 from World Wide Web: http://www.cmcweb.ca/idtheft

Consumer Measures Committee (2004). *Consumer Ministers Advance Initiatives to Protect Consumers in a Marketplace Without Borders.* [Online textfile]. Ottawa: Consumer Measures Committee. Retrieved December 10, 2008 from World Wide Web: http://www.cmcweb.ca/idtheft

Consumer Measures Committee (2005a). *Consumer Identity Theft Kit.* [Online textfile]. Ottawa: Consumer Measures Committee. Retrieved December 10, 2008 from World Wide Web: http://www.cmcweb.ca/idtheft

Consumer Measures Committee. (2005b). *Identity Theft Kit for Business* [Online textfile]. Ottawa: Consumer Measures Committee. Retrieved December 2, 2008 from the World Wide Web: http://www.cmcweb.ca/epic/site/cmc-cmc.nsf/en/fe00091e.html

Consumer Measures Committee (2005c). *Working Together to Prevent Identity Theft: Consultation Workbook* [Online textfile]. Ottawa: Consumer Measures Committee. Retrieved December 10, 2008 from World Wide Web: http://www.cmcweb.ca/idtheft

Consumer Measures Committee (2005d). *Working Together to Prevent Identity Theft: A Discussion Paper* [Online textfile]. Ottawa: Consumer Measures Committee. Retrieved December 10, 2008 from World Wide Web: http://www.cmcweb.ca/idtheft

Consumer Measures Committee (2005e). *Manitobans Invited to Get Involved in Public Consultations* [Online textfile]. Ottawa: Consumer Measures Committee. Retrieved December 10, 2008 from World Wide Web: http://www.cmcweb.ca/idtheft

Consumer Measures Committee (2005f). *National consultation launched on fight against identity theft.* [Online textfile]. Ottawa: Consumer Measures Committee. Retrieved December 10, 2008 from World Wide Web: http://www.cmcweb.ca/idtheft

Craats, R. (2005). *Identity Theft: the scary new crime that targets all of us.* Toronto: Altitude Publishing.

Cruikshank, B. (1999). "Revolutions Within: Self-Government and Self-Esteem." In Cruikshank, B., *The Will to Empower.* New York: Cornell University Press.

D'Amico, M. L. (1998, December 7). Internet has become a necessity, U.S. poll shows. *CNNinteractive* [Internet magazine], p. 1. Retrieved June 20, 1999 from the World Wide Web: http://cnn.com/tech/computing/9812/07/neednet.idg/index.htm [c.f. McKenna & Bargh, 2000].

Dandeker, C. (1990). *Surveillance, Power and Modernity.* Padstow: Polity Press.

Daniel, D., Longbrake, W., & Murphy, N. (1973). The effect of technology on bank economies of scale for demand deposits. *Journal of Finance*, Vol. 28: 131–146.

Dant, T. (2004). The Driver-Car. *Theory, Culture and Society*, Vol. 21(4/5): 61–79.

Degryse, H. (1996). On the interaction between vertical and horizontal product differentiation: An application to banking. *Journal of Industrial Economics*, Vol. 44: 169–186.

Deleuze, G. (1990). Postscript on the Societies of Control. *L'Autre Journal* Vol. 1: 3-7.

Deloitte & Touche LLP. (2008). *Canadian Association of Police Boards: A report on cybercrime in Canada.* Presented April 29, 2008.

Denzin, N.K. (1994). Postmodernism and Deconstructionism. In Carroll, W.K. (ed.), *Critical Strategies for Social Research* (pp. 232-245). Toronto: Canadian Scholar's Press Inc.

Denzin, N.K. & Lincoln, Y.S. (2000). *The SAGE Handbook of Qualitative Research* (2nd ed.). Thousand Oaks, CA: Sage.

Department of Justice (2007). Backgrounder: Distinction between Identity Theft and Identity Fraud [Online textfile]. Ottawa: Department of Justice. Retrieved October 20, 2009 from the World Wide Web: http://canada.justice.gc.ca/eng/news-nouv/nr-cp/2007/doc_32179.html

Department of Justice (2009). Tough New Laws Targeting Identity Theft Receives Royal Assent [Online textfile]. Ottawa: Department of Justice. Retrieved November 2, 2009 from the World Wide Web: http://www.justice.gc.ca/eng/news-nouv/nr-cp/2009/doc_32447.html)

Diener E. (1980) Deindividuation: the absence of selfawareness and self-regulation in group members. In Paulus P.B. (ed.), *The psychology of group influence*. Hillsdale, NJ: Erlbaum.

Du Gay, P. (1996). *Consumption and identity at work*. London: Sage

Duggan, L. (2003) *The Twilight of Equality? Neoliberalism, Cultural Politics, and the Attack on Democracy*. Boston, MA: Beacon Press.

Ekberg, M. (2007). The Parameters of the Risk Society. *Current Sociology*, Vol. 55(3): 343-366.

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

Fairclough, N. (1992). *Discourse and social change*. Cambridge, UK: Polity Press.

Fairclough, N. (1995). *Media Discourse*. London: Edward Arnold.

Fairclough, N. & R. Wodak (1997). Critical Discourse Analysis. In T.A. van Dijk (ed.). *Discourse as Social Interaction*. Discourse Studies: A Multidisciplinary Introduction Volume 2 (2000). London: Sage (pg. 258-284).

Federal Trade Commission .(2003). Overview of the Identity Theft Program: October 1998– September 2003. [Online textfile]. Washington: Federal Trade Commission. Retrieved from World Wide Web: http://www. ftc.gov/os/2003/09/timelinereport.pdf.

Federal Trade Commission. (2006). Consumer Fraud and Identity Theft Complaint Data, January–December 2005, January. [Online textfile]. Washington: Federal Trade Commission. Retrieved from World Wide Web: http://www.consumer. gov/sentinel/pubs/Top10Fraud2005.pdf.

Felson, M. M. (1998). Crime and Everyday Life. Thousand Oaks, CA: Pine Forge.

Ferguson, R. (2000). Information technology in banking and supervision. Remarks at the Financial Services Conference 2000, St. Louis University. St. Louis, Missouri.

Fisher, J.A. (2007). Coming Soon to a Physician Near You: Medical Neoliberalism and Pharmaceutical Clinical Trials. *Harvard Health Policy Review*, Vol. 8(1): 61–70.

Foley, L. (2003). *Identity theft: The aftermath 2003*. Retrieved March 20, 2007, from the Identity Theft Resource Center Web site: http://www.idtheftcenter.org/idaftermath.pdf

Foucault, M. (1979). *Discipline and Punish: the Birth of the Prison*. Harmondsworth: Penguin.

Foucault, M. (1980). *Power/Knowledge. Selected Interviews and other Writings 1972-1977.* Brighton: Harvester.

Foucault, M. (1982). The Subject and Power. In S. Sacks (ed.), *Critical Inquiry*, Vol. 8. Chicago: University of Chicago Press.

Foucault, M. (1988). Technologies of the Self. In L.H. Martin, H. Gutman and P.H. Hutton (eds.), *Technologies of the Self: A Seminar with Michel Foucault.* Amherst: University of Massachusetts: pp. 16-49.

Foucault, M. (1990). *The History of Sexuality, Volume 1: An Introduction* (Robert Hurley Trans.). New York: Vintage Books (Original work published 1977).

Foucault, M. (1991a). Governmentality. In G. Burchell, C. Gordon and P. Miller (eds), *The Foucault Effect: Studies in Governmentality.* London: Harvester Wheatsheaf: pp. 87-104.

Foucault, M. (1991b). Politics and the study of discourse. In G. Burchell, C. Gordon and P. Miller (eds), *The Foucault Effect: Studies in Governmentality.* London: Harvester Wheatsheaf: pp. 53-72.

Foucault, M. (2002). *The Archaeology of Knowledge* (A.M. Smith Trans.). New York: Routledge (Original work published 1969).

Fowler, R. (1985). Ideological Structures in Discourse, in T.A. van Dijk (ed.), *Handbook of Discourse Analysis, Vol. 4* . London: Academic Press (pp. 61-82).

Furnell, S. (2007). Identity Impairment: The problems facing victims of identity fraud. *Computer Fraud & Security*, December 2007: 6-11.

Garland, D. (1997). "'Governmentality' and the problem of crime: Foucault, criminology, sociology." *Theoretical Criminology*, Vol. 1(2): 173-214.

Garland, D. (2001). The Culture of Control: Crime and Social Order in Contemporary Society. Chicago: University of Chicago Press.

Garland, D. (2003). "The Rise of Risk." In Ericson, R. and A. Doyle (eds.), *Risk and Morality.* Toronto: University of Toronto Press.

Garnsey, E., & Rees, B. (1996). Discourse and enactment: Gender inequality in text and context. *Human Relations*, Vol. 49(53): 7-32.

Gaventa, J. & Cornwall, A. (2001). In Carroll, W.K. (ed.), *Critical Strategies for Social Research.* Toronto: Canadian Scholar's Press Inc (pp. 320-333).

Geertz, C. (1973). *The interpretation of cultures.* New York: Basic Books.

General Accounting Office. (2002). Identity theft: Greater awareness and use of existing data are needed. Report to the Honorable Sam Johnson, House of Representatives. Washington, D.C. [GAO-02-766]. Retrieved from the World Wide Web: http://www.consumer.gov/idtheft/reports/gao-d02766.pdf

Gerard, G. J., Hillison, W., & Pacini, C. (2004). Identity theft: The US legal environment and organisations' related responsibilities. *Journal of Financial Crime*, Vol. *12*: 33-43.

Gergen, K. (1999). *An invitation to social construction*. London: Sage.
Grant, D., Keenoy, T. & Oswick, C. (1998). Organizational discourse: Of diversity, dichotomy and multi-disciplinarity. In D. Grant, T. Keenoy, & C. Oswick (eds.). *Discourse and organization.* London: Sage (pp. 1-14).

Giddens, A. (1991). *Modernity and Self-Identity: Self and Society in the Late Modern Age*. Cambridge: Cambridge University Press.

Gies, L. (2008). How material are cyberbodies? Broadband Internet and embodied subjectivity. *Crime Media Culture*, Vol. 4(3): 311-330.

Gilbert, E. (2008). The Art of Governing Smoking: Discourse Analysis of Australian Anti-Smoking Campaigns. *Social Theory & Health*, Vol. 6 : 97-117.

Gill, M. et al. (2006). The fight against identity fraud: a brief study of the EU, the UK, France, Germany, and the Netherlands. Leicester: Perpetuity Research and Consultancy International Ltd.

Giroux, H.A. (2004). *The Terror of Neoliberalism: Authoritarianism and the Eclipse of Democracy*. Boulder, CO: Paradigm Publishers.

Goffman, E. (1959). *The Presentation of Self in Everyday Life*. Garden City: Doubleday Books.

Gordon, C. (1991). "Governmental rationality: an introduction." In G. Burchell, C. Gordon and P. Miller (eds.), *The Foucault Effect: Studies in Governmentality*. Chicago: University of Chicago Press.

Gordon, G.R., Willox, N.A., Rebovich, D.J., Regan, T.M. and Gordon, J.B. (2004). Identity fraud: A critical national and global threat. *Journal of Economic Crime Management*, Vol. 2(1): 1-48.

Grabosky, P. and R. Smith. (2005). Telecommunication Fraud in the Digital Age: the Convergence of Technologies. In D.S. Wall (ed.), *Crime and the Internet*. London; Routledge Publishers.

Graham, E. (2002). *Representations of the Post/Human: Monsters, Aliens and Others in Popular Culture*. New Brunswick: Rutgers University Press.

Graham, S. & Marvin, S. (2001). *Splintering Urbanism: Networked Infrastructures, Technological Mobilities and the Urban Condition*. New York: Routledge.

Habermas, J. (1989). *The Structural Transformation of Public Sphere: An Inquiry into a Category of Bourgeois Society*. Cambridge: MIT Press.

Haggerty, K.D. (2003). From Risk to Precaution: The Rationalities of Personal Crime Prevention. In Ericson, R.V. & Doyle, A. *Risk and Morality*. Toronto: University of Toronto Press (pp. 193–214).

Haggerty, K.D. (2004a). Displaced Expertise: Three constraints on the policy-relevance of criminological thought. *Theoretical Criminology*, Vol. 8 (2): 211-231.

Haggerty, K.D. (2004b). Technology and Crime Policy: Reply to Michael Jacobson. *Theoretical Criminology*, Vol. 8 (4): 491-497.

Haggerty, K.D. (2007). Stolen identities. *Criminal Justice Matters*, 68: 139-40.

Haggerty, K.D. & Ericson, R.V. (2000). The Surveillant Assemblage. *British Journal of Sociology,* Vol. 51(4): 605–22.

Hall, S. (1997). *Representation: Cultural Representations and Signifying Practices.* London: Sage.

Hannah-Moffat, K. (2000). Prisons that Empower. *British Journal of Criminology*, Vol. 40: 510-531.

Hannan, T., & McDowell, J. (1990). The impact of technology adoption on market structure. *Review of Economics and Statistics*, Vol. 72: 164–168.

Harper, J., Singleton, S., 2001. With a grain of salt: what consumer privacy surveys don't tell us. Available online at: http://www.cei.org/PDFs/with_a_grain_of_salt.pdf, accessed on 16 May 2005. Cited from Paine et al. (2007).

Harris. (2004). National Survey on Consumer Privacy Attitudes. Available online at: http://www.epic.org/privacy/survey/, accessed on 22 August 2006. Cited from Paine et al., (2007).

Harvey, A. (2005). *Brief History of Neoliberalism.* Oxford University Press, Oxford.

Hayden, T. (2002). *The Zapatista Reader.* New York: Thunder's Mouth.

Hayles, K.N. (1999). The condition of virtuality. In P. Lunenfeld (ed.), *The digital dialectic: New essays on new media*. Cambridge: MIT Press (pp. 68-95).

Hayward, C.L. (ed.). (2004). *Identity Theft.* New York: Novinka Books.

Henderson, P. (2005). Businesses get wakeup call on identity theft. *Business Edge* 1(25): 1–2.

Heuston, G.H. & Block, J. (2009). The Computer as Significant Other. *FBI Law Enforcement Bulletin* (April 2009): 8-14.

Hiltz S.R., Turoff M., & Johnson K. (1989). Experiments in group decision making, 3: disinhibition, deindividuation, and group process in pen name and real name computer conferences. *Decision Support Systems*, Vol. 5: 217–32.

Hird, J.A. (2005). *Power, Knowledge, and Politics: Policy Analysis in the States.* Washington: Georgetown University Press.

Hinduja, S. (2008). Deindividuation and Internet Software Piracy. *CyberPsychology & Behavior*, Vol. 11(4): 391-398.

Hobbes, T. (1991). *Leviathan*. Cambridge: Cambridge University Press [original work published 1651].

Hoofnagle, C.J. (Fall 2007). Identity Theft: Making the Known Unknowns Known. *Harvard Journal of Law and Technology*, Vol. 21(1): 97-122.

Hoover, K. R. (2003). *Economics as Ideology*. Lanham: Rowman & Littlefield Publishers, Inc.

Horrigan, J.B. (2008). Online Shopping: Internet Users Like the Convenience but Worry About the Security of Their Financial Information. Washington, DC: Pew Internet and American Life Project.

Howard, A. (2005). *Counselling and Identity: Self-Realisation in a Therapy Culture*. New York: Palgrave MacMillan.

Hu, Q. and Dinev, T. (2005). Is spyware an Internet nuisance or public men-ace? Commun. *ACM*, 48, 8 (August): 61–65.

Hughes, Gordon (1998) *Understanding Crime Prevention: Social Control, Risk and Late Modernity*. Buckingham: Open University Press.

Hunter, W., & Timme, S. (1986). Technical change, organizational form and the structure of bank production. *Journal of Money, Credit and Banking*, Vol. 18: 152–166.

Industry Canada (2009). *Mandate* [Online texfile]. Ottawa: Author. Retrieved April 12, 2010 from the World Wide Web: http://www.ic.gc.ca/eic/site/ic1.nsf/eng/h_00018.html#objective1

Industry Canada (2009b). *The Digital Economy in Canada: Trust and Confidence* [Online texfile]. Ottawa: Author. Retrieved May 8, 2010 from the World Wide Web: http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/h_gv00003.html

International Telecommunication Union (2009). *TSB Director's Ad Hoc Group on IPR*. Author: Geneva. [Online textfile]. Retrieved February 6, 2008 from World Wide Web: http://www.itu.int/ITU-T/othergroups/ipr-adhoc/openstandards.html

Jackson, B.G. (2000). A fantasy theme analysis of Peter Senge's *Learning Organization. Journal of Applied Behavioral Science*, Vol. 36: 193-209.

Jacobson, M. (2004). Reply to Kevin D. Haggerty. *Theoretical Criminology,* Vol. 8(2): 233–238.

Javelin Strategy & Research (2007). 2007 Identity Fraud Survey Report: Identity Fraud is Dropping, Continued Vigilance Necessary. February. A shortened complimentary version of the Javelin report can be obtained at http://www.javelinstrategy.com/uploads/701.R_2007IdentityFraudSurveyReport_Brochure.pdf.

Jessop, B. (1995). The Regulation Approach, Governance and Post-Fordism: Alternative Perspectives on Economic and Political Change?. *Economy and Society*, 24: 307-333.

Jewkes, Y. (2003) Policing the Net: Crime, Regulation and Surveillance in Cyberspace. In Y. Jewkes (ed.), *Dot.Cons: Crime, Deviance and Identity on the Internet*. Portland: Willan Publishing (pp. 15-35).

Johnson, R. D., & Downing, L. L. (1979). Deindividuation and valence of cues: Effects on prosocial and antisocial behavior. *Journal of Personality and Social Psychology,* Vol. 37: 1532–1538.

Jones, R. (2000). Digital rule: Punishment, control and technology. *Punishment and Society*, Vol. 2(1): 5-22.

Jordan, B. (1985). *The State: Authority and Autonomy*. Oxford: Basil Blackwell Publishing.

Kahn, C. & Roberds, W. (2005). Credit and Identity Theft. *Federal Reserve Bank of Atlanta Working Paper,* 2005-19.

Karjaluoto, H., Koivumaki, T. & Salo, J. (2003). Individual differences in private banking: empirical evidence from Finland. Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS). Big Island: Hawaii, 196.

Katz, C. (2006). The State Goes Home: Local Hypervigilance of Children and the Global Retreat from Social Reproduction. In T. Monahan (ed.) *Surveillance and Security: Technological Politics and Power in Everyday Life*. New York: Routledge (pp. 27–36).

Keenoy, T., Oswick, C. & Grant, D. (1997). Organizational discourse: Text and context. *Organization,* 2: 147-158.

Kennett, P. (ed.). (2008). *Governance, Globalization and Public Policy*. Cheltenham: Edward Elgar Publishers Ltd.

Kiesler, S. (1986). The hidden messages in computer networks. *Harvard Business Review* (January–February).

Kinchloe, J. & McLaren, P. (1994). Rethinking critical theory and qualitative research. In N. Denzin & Y. Lincoln (eds.). *Handbook of Qualitative Research.* Thousand Oaks, CA: Sage (pp. 138-157).

Kingdon, J.W. (1984). *Agendas, Alternatives, and Public Policies*. Boston: Little, Brown and Company Ltd.

Klineberg, J. (2009). Proceedings from the Standing Committee on Justice and Human Rights, 40th Parliament, 2nd Session (September 17). Ottawa: Ontario.

Knoepfel, P., Larrue, C., Varone, F. & Hill, M. (2007). *Public Policy Analysis.* Bristol, UK: The Policy Press.

Koops, Bert-Jaap, Leenes, R., Meints, M., van der Meulen, N. & Jaquet-Chiffelle, D.O. (2009). A Typology of Identity-Related Crime. *Information, Communication & Society*, 12(1): 1-24.

Koops, B. J. & Leenes, R. E. .(2006). ID theft, ID fraud and/or ID-related crime. Definitions matter. *Datenschutz und Datensicherheit.* Vol. 30 (9): 553–556.

Kraft, M.E. & S.R. Furlong (2007). *Public Policy: Politics, Analysis, and Alternatives* (2nd ed.). Washington: CQ Press.

Kress, G. (1985). Ideological Structures in Discourse, in T.A. van Dijk (ed.), *Handbook of Discourse Analysis, Vol. 4*: 27-42.

Kroger, J. (2000). *Identity Development: Adolescence Through Adulthood.* Thousand Oaks: Sage Publications, Inc.

Lacey, D. & Cuganesan, S. (2004). The Role of Organizations in Identity Theft Response: The Organization—Individual Victim Dynamic. *The Journal of Consumer Affairs*, Vol, 38 (2): 244-261.

Larkin, E. (2009). Security Alert: Organized Crime Moves Into Data Theft. *PCWorld.com.* (July 2009): 33-34.

Larose, R., Rifon, N.J. & Ebody, R. (2008). Promoting Personal Responsibility for Internet Safety. *Communications of the ACM.* Vol. 51 (3): 71-76.

Lash, S. (2001). Technological Forms of Life. *Theory, Culture and Society,* Vol. 18(1): 105–120.

Latour, B. (1991). Technology Is Society Made Durable. In J. Law (ed.). *A Sociology of Monsters.* London: Routledge: 103–31.

Levenson, J.R. (2008). Strength in Numbers: An Examination into the Liability of Corporate Entities for Consumer and Employee Data Breaches. *University of Florida Journal of Law and Public Policy*, Vol. 19: 95-123.

Lewis, J. (2002). *Cultural Studies: The Basics.* London: Sage Publishers.

Locke, T. (2004). *Critical Discourse Analysis.* London: Continuum.

Los, M. (2006). Looking into the future: Surveillance, globalization and the totalitarian potential. In D. Lyon (ed.). *Theorizing surveillance: The panopticon and beyond.* Portland: Willan Publishing: 69-94.

Loseke, D.R. (2003). *Thinking about social problems* (2nd ed.). Hawthorne, NY: Aldine de Gruyter.

Lyon, D. (2006). Airport screening, surveillance and social sorting: Canadian Responses to 9/11 in context. *Canadian Journal of Criminology and Criminal Justice*. Vol. 48(3): 397-411.

Main, G. & Robson, B. (2001). *Scoping Identity Fraud*. Canberra: Commonwealth Attorney-General's Department.

Marcus, G.E. (1994). What comes (just) after "post"? The case of ethnography. In N.K. Denzin & Y.S. Lincoln (eds.). *Handbook of qualitative research*. London: Sage (pp. 563-574).

Marin, B. (1990). "Generalized Political Exchange: Preliminary Considerations" in B. Marin (ed.), *Generalized Political Exchange: Antagonistic Cooperation and Integrated Policy Circuits*. Frankfurt: Campus Verlag.

Marshall, A.M. and B.C. Tompsett. (2005). "Identity Theft in an Online World." *Computer Law and Security Report*, Vol. 21: 128-137.

Martinez, E. & Garcia, A. (1997). *What is Neo-liberalism: A Brief Definition for Activists*. Retrieved 1 April 2009 from World Wide Web: http://www.corpwatch.org/article.php?id=376

Marvasti, A. (2004). *Qualitative Research in Sociology*. London: Sage Publications.

Marx, G.T. (1995). The Engineering of Social Control: The Search for the Silver Bullet. In J. Hagan and R. Peterson (eds). *Crime and Inequality*. Stanford: Stanford University Press (pp. 225-246).

May, D.A. & J.E. Headley (2004). *Identity Theft*. New York: Peter Lang Publishing.

Mayer, E. (2005). *ID theft victims face lots of work*. http://www.contracostatimes.com/mld/cctimes/business/personal_finance/11071320.

McKenna, K.Y.A. & Bargh, J.A. (2000). Plan 9 from Cyberspace: The Implications of the Internet for Personality and Social Psychology. *Personality and Social Psychology Review*, Vol. 4(1): 57-75.

McKenna, K.Y.A., Green, A.S., & Gleason, M.E.J. (2002). Relationship Formation on the Internet: What's the Big Attraction? *Journal of Social Issues*, Vol. 58(1): 9-31.

McWaters, G. & Ford, G. (2007). *The Canadian Guide to Protecting Yourself from Identity Theft and Other Fraud*. Toronto: Insomniac Press.

Mendels, P. (1999, July 21). The two faces of on-line anonymity. *New York Times* [Internet edition]. Available: http://www.nytimes.com/library/tech/99/07/cyber/articles/21anonymity.html

Mey, J. (1985). *Whose Language: A Study in Linguistic Pragmatics*. Amsterdam: Benjamins.

Miles, M.B. & Huberman, A.M. (1994). *Qualitative Data Analysis: An Expanded Sourcebook*. London: Sage.

Mill, J.S. (2006). *On Liberty and the Subjectification of Women*. New York: Penguin Books [Original work published 1859].

Miller, P. & Rose, N. (1990). Governing Economic Life. *Economy and Society*, Vol. 19(1): 1–31.

Miller, P. & Rose, N. (1992). Political Power Beyond the State: Problematics of Government. *British Journal of Sociology*, Vol. 43 (2): 172-205.

Milne, G.R. (2003). How Well Do Consumers Protect Themselves from Identity Theft? *The Journal of Consumer Affairs*, Vol. 37(2): 388-402.

Mitchison, N., Wilikens, M., Breitenbach, L., Urry, R. & Portesi, S. (2004). *Identity Theft—A Discussion Paper*. European Commission Directorate General Joint Research Centre (Unrestricted).

Monahan, T. (2009). Identity theft vulnerability: Neoliberal governance through crime construction. *Theoretical Criminology*, Vol. 13(2): 155-176.

Moneris Solutions. (2006). Canada's Credit and Debit Card Processing Experts 2006 http://www.bcroyalbank.com/merchantservices.

More Americans Fear Cybercrime Than Physical Crime, According to IBM Study. (2006). *Criminal Law Reporter, Vol. 78*: 725.

Muller, P. (1990). *Les politiques publiques*. Paris: Presses Universitaires de France.

National Research Council of Canada (2007). Data and Text Mining. Author: Ottawa. [Online textfile]. Retrieved January 14, 2009 from World Wide Web: http://iit-iti.nrc-cnrc.gc.ca/r-d/ai-data-mining-exploration-donnees-ia_e.html

Newman, G.R. & McNally, M.M. (2005). *Identity Theft Literature Review*. Report Presented to Department of Justice January 27-28, 2005. Unpublished.

Newman, G.R, and R. Clarke (2003). *Superhighway Robbery: Preventing E-Commerce Crime*. London: Willan.

Norris, C. & McCahill, M. (2006). CCTV: Beyond Penal Modernism. *British Journal of Criminology*, Vol. 46: 97-118.

O'Malley, P. (1992). Risk, Power and Crime Prevention. *Economy & Society*, 21 (3): 252-275.

O'Malley, P. (1996). Risk and Responsibility. In Barry, A., Osborne, T. & Rose, N. (eds.). *Foucault and Political Reason: Liberalism, Neo-Liberalism and Rationalities of Government*. Chicago: University of Chicago Press (pp. 189–207).

O'Malley, P. (1998). *Crime and the Risk Society*. Aldershot: Ashgate.

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

O'Malley, P. (2008). Experiments in Risk and Criminal Justice. *Theoretical Criminology*, Vol. 12 (4): 451-469.

O'Malley, P., L. Weir, & C Shearing (1997). "Governmentality, Criticism, Politics" in *Economy and Society* 26, 4.

Olstead, R. (2002). Contesting the text: Canadian media depictions of the conflation of mental illness and criminality. *Sociology of Health and Illness*, 24 (5), pp. 621-643.

Organisation for Economic Co-operation and Development (2008). *Scoping Paper on Online Identity Theft*. Ministerial Background Report DSTI/CP(2007)3/FINAL. Presented June 17-18, 2008 in Seoul Korea at OECD Ministerial Meeting on the Future of the Internet Economy.

Ovum (2006) International Broadband Market Comparisons. Retrieved August 10, 1997 from World Wide Web: http://www.ovum.com [c.f. Gies, 2008].

Paine, C., Relps, U.D., Stieger, S. Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies*, Vol, 65 (6): 526-536.

Pal, L.A. (1992). *Public Policy Analysis: An Introduction* (2nd ed.). Scarborough: Nelson Canada.

Palys, T. & Atchison, C. (2008). *Research Decisions: Quantitative and Qualitative Perspectives* (4th ed.). Toronto: Nelson Education Ltd.

Parker, I. (1992). *Discourse dynamics*. London: Routledge.

Pease, K. (2005). "Crime Futures and Foresight: Challenging Criminal Behaviour in the Information Age." In D.S. Wall (ed.) *Crime and the Internet*. London: Routledge Publishers.

Pedwell, T. (2007, November 22). Identity-theft proposal hailed as a first step. *Toronto Star*. [Newspaper, selected stories online]. Retrieved January 15, 2009 from World Wide Web: http://www.thestar.com/article/278914

Pennathur, A.K. (2001). 'Clicks and bricks': e-Risk Management for banks in the age of the Internet. *Journal of Banking and Finance*, Vol. 25: 2103-2123.

Perrow, C. (1984). *Normal Accidents: Living with High-Risk Technologies*. New York: Basic Books.

Peters, B.G. (2006). "Contracts and Resource Allocation in Public Governance," in A. Heritier (ed.), *Common Goods: Reinventing European and International Governance*. Lanham: Rowman and Littlefield.

Peters, B.G. & J. Pierre (eds.). (2006). *Handbook of Public Policy*. London: Sage Publications.

Phillips, N. & Brown, J. (1993). Analyzing communcation in and around organizations: A critical hermeneutic approach. *Academy of Management Journal*, Vol. 36:1547-1576.

Phillips, L. and Jorgensen, M.W. (2002). *Discourse Analysis as Theory and Method*. London: Sage Publications.

Phillips, N. & Ravasi, D. (1998, July). *Analyzing social construction in organizations: Discourse analysis as a research method in organization and management theory*. Paper presented at the Third International Conference on Organizational Discourse: Pretexts, Subtexts and Contexts, London.

Phonebusters (2009). *Statistics on Phone Fraud*. Author: North Bay. [Online textfile]. Retrieved October 22, 2009 from World Wide Web: http://www.phonebusters.com/english/statistics.html

Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5.

Pierre, J. & B.G. Peters (eds.). (2000). *Governance, Politics and the State*. New York: St. Martin's Press.

Pikkarainen, T., Pikkarainen, K., Karjaluoto, H., & Pahnila, S. (2004). Consumer acceptance of online banking: an extension of the technology acceptance model. *Internet Research*, Vol. 14 (3): 224-235.

Pontell, Henry N. 2009. Identity theft: Bounded rationality, research, and policy. *Criminology & Public Policy,* Vol. 8 (2).

Poster, M. (1990). *The mode of Information: poststructuralism and social context*. Chicago: Polity Press.

Postmes T., Spears R., & Lea M. Breaking or building social barriers: a SIDE analysis of computer-mediated communication. *Communication Research*, Vol. 25: 689–715.

Poston, R., Stafford, T.F. & Hennington, A. (2005). Spyware: A view from the (online) street. Commun. *ACM* 48, 8 (Aug): 96–99.

Potter, J. (1997). Discourse Analysis as a Way of Analyzing Naturally Occuring Talk. In D. Silverman (ed.), *Qualitative Research: Theory, Method and Practice*. London/Thousand Oaks: Sage Publications.

Potter, J. (2004). Discourse analysis as a way of analyzing naturally-occurring talk. In D. Silverman (ed.), *Qualitative Research: Theory, Method and Practice* (2nd Ed.). London: Sage Publishers: 200-21.

Public Safety Canada. (2008). *Identity Theft – Questions and Answers* [Online textfile]. Ottawa: Author. Retrieved December 1, 2008 from the World Wide Web: http://www.safecanada.ca/identitytheft_e.asp

Pullen, A., N. Beech, & D. Sims (eds.). (2007). *Exploring Identity: Concepts and Methods*. New York: Palgrave MacMillan.

Rajchman, J. (1991). *Truth and Eros: Foucault, Lacan and the Question of Ethics*. New York: Routledge.

Rapley, T. (2007). *Doing Conversation, Discourse and Document Analysis*. Thousand Oaks, CA: Sage Publications.

Rasmussen, D.M. (ed.) (1996). *The Handbook of Critical Theory*. Oxford: Blackwell.

Reissman, C. (1993). *Narrative Analysis*. London: Sage.

Rigakos, G.S. & Hadden, R.W. (2001). Crime, capitalism and the 'risk society': Towards the same olde modernity? *Theoretical Criminology*, Vol. 5(1): 61-84.

Riggins, S.H. (1997). The rhetoric of othering. In S.H. Riggins (ed.), *The language and politics of exclusion*. Thousand Oaks, CA: Sage (pp. 1-30).

Ritchie, J. & Spencer, L. (1994). Qualitative data analysis for applied policy research. In A. Bryman & R.G. Burgess (eds.). *Analyzing Qualitative Data*. London: Routledge (pp. 77-108).

Ritchie, J., Lewis, J. & Elam, G. (2003). Designing and Selecting Samples. In J. Ritchie & J. Lewis (eds.), *Qualitative Research Practice*. Thousand Oaks, CA: Sage.

Rose, N. (1993). Government, Authority and Expertise in Advanced Liberalism. *Economy and Society* 22/3: 283-300.

Rose, N. (1996a). *Inventing Ourselves: Psychology, Power, and Personhood*. Cambridge: Cambridge University Press.

Rose, N. (1996b). The Death of the Social? Re-figuring the Territory of Government. *Economy and Society* 24, 3: 327-356.

Rose, N. (1999). *Powers of Freedom: Reframing Political Thought*. Cambridge: Cambridge University Press.

Rose, N. (2000). Government and Control. In D. Garland and R. Sparks (eds.), *Criminology and Social Theory*. Oxford: Clarendon Press.

Royal Bank of Canada (2008a). *Electronic Access Agreement*. Royal Bank of Canada: Toronto. [Online textfile]. Retrieved January 7, 2010 from World Wide Web: https://www.rbcroyalbank.com/onlinebanking/terms_08.html

Royal Bank of Canada (2008b). *Financial Fraud* (03/2008). [Brochure]. Royal Bank of Canada: Toronto.

Royal Bank of Canada (2009a). *Client Agreement – Client Card and Personal Identification Number* [10/2009]. [E-Form 1672]. Royal Bank of Canada: Toronto.

Royal Bank of Canada (2009b). *Personal banking and savings accounts* [02/2009]. [Brochure]. Royal Bank of Canada: Toronto.

Royal Bank of Canada (2009c). *Protecting Your Privacy* [09/2009]. [Brochure]. Royal Bank of Canada: Toronto.

Royal Bank of Canada (2009d). *Royal Bank of Canada*. Royal Bank of Canada: Toronto. [Online textfile]. Retrieved February 2, 2009 from World Wide Web: http://www.rbc.com

Royal Bank of Canada (2009e). *Royal Bank of Canada: Corporate Profile*. Royal Bank of Canada: Toronto. [Online textfile]. Retrieved February 2, 2009 from World Wide Web: http://www.rbc.com

Royal Bank of Canada (2009f). *Royal Bank of Canada: Investor Relations*. Royal Bank of Canada: Toronto. [Online textfile]. Retrieved February 2, 2009 from World Wide Web: http://www.rbc.com/investorrelations/pdf/qf_q4_08.pdf

Royal Bank of Canada. (2010a). *Communicating with Us Safely*. Royal Bank of Canada: Toronto. [Online textfile]. Retrieved January 7, 2010 from World Wide Web: http://www.rbc.com/privacysecurity/ca/communicating-with-us-safely.html

Royal Bank of Canada. (2010b). *Email & Website Fraud*. Royal Bank of Canada: Toronto. [Online textfile]. Retrieved January 7, 2010 from World Wide Web: http://www.rbc.com/privacysecurity/ca/email-and-website-fraud-1.html

Royal Bank of Canada. (2010c). *How RBC Helps to Protect You Against Fraud*. Royal Bank of Canada: Toronto. [Online textfile]. Retrieved January 7, 2010 from World Wide Web: http://www.rbc.com/privacysecurity/ca/how-rbc-helps-to-protect-you-against-fraud.html

Royal Bank of Canada. (2010d). *How We Use Your Information*. Royal Bank of Canada: Toronto. [Online textfile]. Retrieved January 7, 2010 from World Wide Web: http://www.rbc.com/privacysecurity/ca/how-we-use-your-information.html

Royal Bank of Canada. (2010e). *Identity Theft*. Royal Bank of Canada: Toronto. [Online textfile]. Retrieved January 7, 2010 from World Wide Web: http://www.rbc.com/privacysecurity/ca/identity-theft.html

Royal Bank of Canada. (2010f). *Legal Terms of Use*. Royal Bank of Canada: Toronto. [Online textfile]. Retrieved February 2, 2010 from World Wide Web: http://www.rbc.com/legal/

Royal Bank of Canada (2010g). *Online Banking Security Features*. Royal Bank of Canada: Toronto. [Online textfile]. Retrieved February 2, 2010 from World Wide Web: http://www.rbcroyalbank.com/RBC:SYoft471A8UAaAboOAI/onlinebanking/bankingusertips/security/features.html#1

Royal Bank of Canada. (2010h). *Online Banking Security Guarantee*. Royal Bank of Canada: Toronto. [Online textfile]. Retrieved February 2, 2010 from World Wide Web: http://www.rbcroyalbak.com/online/rbcguarantee.html

Royal Bank of Canada. (2010i). *Online Privacy*. Royal Bank of Canada: Toronto. [Online textfile]. Retrieved January 7, 2010 from World Wide Web: http://www.rbc.com/privacysecurity/ca/online-privacy.html

Royal Bank of Canada. (2010j). *Privacy & Security Canada*. Royal Bank of Canada: Toronto. [Online textfile]. Retrieved January 7, 2010 from World Wide Web: http://www.rbc.com/privacysecurity/ca/

Royal Bank of Canada. (2010k). *Protecting Your Computer*. Royal Bank of Canada: Toronto. [Online textfile]. Retrieved January 7, 2010 from World Wide Web: http://www.rbc.com/privacysecurity/ca/protecting-your-computer.html

Royal Bank of Canada. (2010l). *Protecting Your Information*. Royal Bank of Canada: Toronto. [Online textfile]. Retrieved January 7, 2010 from World Wide Web: http://www.rbc.com/privacysecurity/ca/protecting-your-information.html

Royal Bank of Canada. (2010m). *Protect Your Identity*. Royal Bank of Canada: Toronto. [Online textfile]. Retrieved January 7, 2010 from World Wide Web: http://www.rbc.com/privacysecurity/ca/protect-your-identity.html

Royal Bank of Canada. (2010n). *Remember to Log Off*. Royal Bank of Canada: Toronto. [Online textfile]. Retrieved January 7, 2010 from World Wide Web: http://www.rbc.com/privacysecurity/ca/remember-to-log-off.html

Royal Bank of Canada. (2010o). *Report ID Fraud*. Royal Bank of Canada: Toronto. [Online textfile]. Retrieved January 7, 2010 from World Wide Web: http://www.rbc.com/privacysecurity/ca/report-id-fraud.html

Royal Bank of Canada. (2010p). *Schemes & Scams*. Royal Bank of Canada: Toronto. [Online textfile]. Retrieved January 7, 2010 from World Wide Web: http://www.rbc.com/privacysecurity/ca/schemes-and-scams.html

Royal Bank of Canada. (2010q). *Securing Your Passwords*. Royal Bank of Canada: Toronto. [Online textfile]. Retrieved January 7, 2010 from World Wide Web: http://www.rbc.com/privacysecurity/ca/securing-your-passwords.html

Royal Bank of Canada. (2010r). *Sharing Your Information*. Royal Bank of Canada: Toronto. [Online textfile]. Retrieved January 7, 2010 from World Wide Web: http://www.rbc.com/privacysecurity/ca/sharing-your-information.html

Royal Bank of Canada. (2010s). *Spyware & Unwanted Software*. Royal Bank of Canada: Toronto. [Online textfile]. Retrieved January 7, 2010 from World Wide Web: http://www.rbc.com/privacysecurity/ca/spyware-and-unwanted-software.html

Royal Bank of Canada. (2010t). *Steps for Safe Computing*. Royal Bank of Canada: Toronto. [Online textfile]. Retrieved January 7, 2010 from World Wide Web: http://www.rbc.com/privacysecurity/ca/steps-for-safe-computing.html

Royal Bank of Canada. (2010u). *Test Your Computer.* Royal Bank of Canada: Toronto. [Online textfile]. Retrieved January 7, 2010 from World Wide Web: http://www.rbc.com/privacysecurity/ca/test-your-computer.html

Royal Bank of Canada. (2010v). *Using a Firewall.* Royal Bank of Canada: Toronto. [Online textfile]. Retrieved January 7, 2010 from World Wide Web: http://www.rbc.com/privacysecurity/ca/using-a-firewall.html

Royal Bank of Canada. (2010w). *Using Anti-Virus Software.* Royal Bank of Canada: Toronto. [Online textfile]. Retrieved January 7, 2010 from World Wide Web: http://www.rbc.com/privacysecurity/ca/using-anti-virus-software.html

Royal Bank of Canada. (2010x). *What Information We Collect.* Royal Bank of Canada: Toronto. [Online textfile]. Retrieved January 7, 2010 from World Wide Web: http://www.rbc.com/privacysecurity/ca/what-information-we-colect.html

Saffran, D. (2005). *Canadians and identity theft: Concern on the rise.* Available at: http://www.ccnmatthews.com/news/releasesfr/show.jsp?action1⁄4showrelease&actionfor

Samarajiva, R. & Shield, P. (1992) Emergent institutions of the "intelligent network": Toward a theoretical understanding. *Media, Culture and Society*, 14: 397–419.

Schneier, B. (2004) *Secrets and Lies: Digital Security in a Networked World* (1st ed.). new York: John Wiley & Sons.

Schoudt, E.M. (2002). "Identity Theft: Victims 'Cry Out' for Reform." *American University Law Review* 52: 339-392.

Schreft, S. L. (2007). Risks of identity theft: Can the market protect the payment system?, *Economic Review*, Federal Reserve Bank of Kansas City, Fourth Quarter: 5–40.

Schutz, A. (1970). *On Phenomenology and Social Relations* (ed. & trans. H.R. Wagner). Chicago: University of Chicago Press.

Schwandt, T.A. (1994). Constructivist, interpretivist approaches to human inquiry. In N.K. Denzin & Y.S. Lincoln (eds.), *Handbook of qualitative research.* Thousand Oaks, CA: Sage (pp. 118-137).

Schwartz, P. (1999). Privacy and Democracy in Cyberspace. *Vanderbilt Law Review*, 2052: 1609-1705.

Shoudt, E. M. (2002). Identity Theft: Victims 'Cry Out' For Reform. *American University Law Review* 52: 339-392.

Sikka, P. (2006). The internet and possibilities for counter accounts: some reflections. *Accounting, Auditing & Accountability Journal*, Vol. 19 (5): 759-69.

Simon, J. (2006). *Governing through Crime: How the War on Crime Transformed American Democracy and Created a Culture of Fear.* New York: Oxford University Press.

Smith, A. (2000). *The Wealth of Nations.* New York: Modern Library [Original work published 1790].

Snape, D. & Spencer, L. (2003). The Foundations of Qualitative Research. In J. Ritchie & J. Lewis (eds.), *Qualitative Research Practice.* Thousand Oaks, CA: Sage (pp.1-23).

Solove, D.J. (2004). *Technology and Privacy in the Information Age.* New York: NYU Press.

Solove, D.J. (2007). Telephone conversation between Daniel Solove, Assoc. Professor of Law, George Washington University Law Sch. and Chris Hoofnagle (Feb. 6, 2007). Cited from Hoofnagle (2007).

South, N. (1987). The Security and Surveillance of the Environment. In John Lowman, Robert Menzies and T. Palys (eds.) *Transcarceration: Essays in the Sociology of Social Control.* Aldershot (pp. 139–52).

Spears, R., Postmes, T., Lea, M. & Wolbert, A. (2002). When Are Net Effects Gross Products: The Power of Influence and the Influence of Power in Computer-Mediated Communication. *Journal of Social Issues*, Vol. 58(1): 91-107.

Spector, M. & Kitsuse, J.I. (1977). *Constructing social problems.* Menlo Park, CA: Cummings.

Spencer, L., Ritchie, J. & O'Connor, W. (2003). Analysis: Practices, Principles and Processes. In J. Ritchie & J. Lewis (eds.), *Qualitative Research Practice.* Thousand Oaks, CA: Sage (pp. 199-218).

Stana, R. (2002). Awareness and Use of Existing Data on Identity Theft. In C.L. Hayward (ed.). *Identity Theft.* New York: Novinka Books.

Statistics Canada, 2006. Available online at: http://ca.today.reuters.com/news/newsArticle.aspx?type=technologyNews&storyID=2006-08-16T062630Z_01_N16412854_RTRIDST_0_TECH-MEDIA-CANADA-COL.XML, accessed on August 22. Cited from Paine et al. (2007).

Statistics Canada (2008a). The Canadian Internet Use Survey. *The Daily June 12, 2008* [Online textfile]. Ottawa: Retrieved November 22, 2008 from the World Wide Web: http://www.statcan.gc.ca/daily-quotidien/080612/dq080612b-eng.htm

Statistics Canada (2008b). E-commerce: Shopping on the Internet. *The Daily November 17, 2008.* Author: Ottawa [Online textfile]. Retrieved May 8, 2010 from the World Wide Web: http://www.statcan.gc.ca/daily-quotidien/081117/dq081117a-eng.htm

Steeves, V. & Wing, C. (2006). Canada's Internet Generation: Connected, Active and Younger Than Ever. *School Libraries in Canada* (pp. 7-13).

Story, L. (2008, March 10). To Aim Ads, Web is Keeping Closer Eye on You. *New York Times* [Newspaper, selected stories online[. Retrieved February 12, 2009 from World Wide Web: http://www.nytimes.com/2008/03/10/technology/10privacy.html?_r=2

Strauss, A. & Corbin, J. (1998). *Basic of Qualitative Research: Techniques and Procedures for Developing Grounded Theory* (2nd ed.). Thousand Oaks, CA: Sage Publications.

Taylor, S. (2001). Locating and Conducting Discourse Analytic Research. In M. Wetherell, S. Taylor, & S.J. Yates (eds.). *Discourse as Data: A Guide for Analysis.* London: Sage Publications.

Synovate. (2003). *Federal Trade Commission: Identity Theft Survey Report.* McLean, VA. Retrieved February 6, 2010 from World Wide Web: http://www.ftc.gov/os/2003/09/synovatereport.pdf

Toulmin, S.E. (1958). *The uses of argument.* Cambridge, UK: Cambridge University Press.

Townley, B. (1993). Foucault, power/knowledge and its relevance for human resource management. *Academy Management Review*, 18, 518-545.

Turner, M. (2001). Emphasis Put on the 'Triple Bottom Line.' *Financial Times* [London], February 8.

Tyler, T. (2002). Is the Internet Changing Social Life? It Seems the More Things Change, the More They Stay the Same. *Journal of Social Issues*, Vol. 58(1): 195-205.

U.S. Public Law 105-318 (1998, October 30). 105th Cong.112 Stat. 3007. *Identity Theft Assumption and Deterrence Act of 1998.*

Van der Meulen, N. (2006). The challenge of countering identity theft: recent developments in the United States, the United Kingdom, and the European Union. Tilburg: Author. [Online textfile]. Retrieved from World Wide Web: http://www.tilburguniversity.nl/intervict/publications/NicolevanderMeulen.pdf

Van Dijk, T.A. (1997). Discourse as Interaction in Society. In T.A. van Dijk (ed.). *Discourse as Social Interaction.* Discourse Studies: A Multidisciplinary Introduction Volume 2 (2000). London: Sage (pg. 1-37).

Van Heffen, O., W.J.M. Kickert, & J.J.A. Thomassen (eds.). (2000). *Governance in Modern Society: Effects, Change and Formation of Government Institutions* (Vol. 4). Dordrecht: Kluwer Academic Publishers.

Van Leeuwen, T. (2008). *Discourse and Practice: new Tools for Critical Discourse Analysis.* New York: Oxford.

Wacquant, L. (2001). Deadly Symbiosis: When Ghetto and Prison Meet and Mesh. *Punishment & Society*, Vol. 3(1): 95–134.

Wall, D.S. (ed.). (2001). *Crime and the Internet.* London: Routledge Publishers.

Wall, D.S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press.

Weber, M. (1968). The interpretive understanding of social action. In M. Brodbeck (ed.), *Readings in the Philosophy of the social sciences*. New York: MacMillan (pp. 85-97). (Reprinted from M. Weber, 1949, *The Methodology of the social sciences*, New York: The Free Press.)

Weber, M. (1977). *The Theory of Social and Economic Organization*. New York: Free Press.

Weedon, C. (1987). *Feminist Practice and Poststructuralist Theory*. Oxford: Blackwell.

Weiss, J. (1989). The Powers of Problem Definition: The Case for Government Paperwork. *Policy Sciences*, Vol. 22.

Wheelock, D., & Wilson, W. (1999). Technical progress, inefficiency, and productivity change in US banking, 1984–1993. *Journal of Money, Credit and Banking*, Vol. 31: 212–234.

White, M.D. & Fisher, C. (2008). Assessing Our Knowledge of Identity Theft: The Challenges to Effective Prevention and Control Efforts. *Criminal Justice Policy Review*, Vol. 19(1): 3-24.

Whitson, J.R. (2009). Identity Theft and the Challenges of Caring for Your Virtual Self. *Interactions*, March-April: 41-45.

Whitson, J.R. & K.D. Haggerty. (2008). Identity Theft and the Care of the Virtual Self. *Economy and Society,* Vol. 37(4): 572-594.

Winner, L. (1977). *Autonomous Technology: Technics-Out-of-Control as a Theme in Political Thought*. Cambridge: MIT Press.

Winner, L. (1986). *The Whale and the Reactor: A Search for Limits in an Age of High Technology*. Chicago, IL: University of Chicago Press.

Winterdyk, J. and Thompson, N. (2008). Student and Non-student Perceptions and Awareness of Identity Theft. *Canadian Journal of Criminology and Criminal Justice* (April 2008), Vol. 50 (2): 153-186.

Witte, K. (1992). Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model. *Communication Monographs*, Vol. 59 (4): 41-43.

Wood, L.A. & Kroger, R.O. (2000). *Doing Discourse Analysis: Methods for Studying Action in Talk and Text*. Thousand Oaks, CA: Sage Publications.

Woodilla, J. (1998). Workplace conversations: The text of organizing. In D. Grant, T. Keenoy, & C. Oswick (eds.). *Discourse and organization*. London: Sage (pp. 31-50).

Yin, R.K. *Case Study Research: Design and Methods* (Rev. ed.). Newbury Park, CA:

Sage Publications.

Young, K.(1998).*Caught in the Net: How to recognize the signs of Internet addiction and a winning strategy for recovery*. New York: Wiley.

Zimbardo, P. G. (1969). The human choice: Individuation, reason, and order vs. deindividuation, impulse and chaos. In W. J. Arnold & D. Levine (eds.), *Nebraska Symposium on Motivation,* Vol. 17: 237–307.

Zureik, E. & M.B. Salter (eds.). (2005). *Global Surveillance and Policing: Borders, Security, Identity*. Portland: Willan Publishing.