The Securitization and Commodification of the Consumer-Citizen: Biopolitics of the Credit Card Industry

by

Katrina Nyyssonen

A thesis

presented to the University Of Waterloo

in fulfilment of the

thesis requirement for the degree of

Master of Arts

in

Sociology

Waterloo, Ontario, Canada, 2018

Author's declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

This thesis examines the biopolitics of the credit card industry and its governance of consumers through consumer-citizenship obligations and the transformation of consumer data into valuable information commodities. Biometrics and transactional data trails or 'data doubles' are used to securitize identity, define responsible citizenship, and to delimit rights and access to valuable social resources. Binding data to consumer-citizens enables the credit card industry to exercise biopower over consumer subpopulations through social sorting based on categories of risk and value. Subpopulations are then both acted upon and sold to third parties as 'valuable information commodities.' This thesis analyzes Visa and Mastercard Canadian credit card policies to determine how the consumer-citizenship is constituted and the extent to which Canadian federal legislation (Personal Information Protection and Electronic Documents Act enable) enables or constrain credit card companies exercise of biopower over consumer populations. This thesis concludes that credit card companies enact a form of biopolitical governance-at-a-distance through entrepreneurship and responsibilization. Corporate policies enable the aggregation and commodification of personal information, for purposes not explicitly made known to customers, in order to drive economic growth for the credit card industry and its 'third parties.'

Acknowledgements

I would first like to thank my thesis advisor Dr. Daniel O'Connor of the Department of Sociology and Legal Studies at the University of Waterloo. Prof. O'Connor was always supportive, very patient and provided his expert knowledge and guidance. I am very grateful for Prof. O'Connor encouraging me to complete my Master's and I was blessed to have him as my advisor.

I would also like to thank the rest of my thesis committee: Dr. Kate Henne and Dr. Philip Boyle for their time, and insightful comments and questions.

In addition, I would like to thank my parents for their sacrifice and encouragement, and Jesus Christ my Lord and saviour for giving me strength and perseverance.

Table of Contents

1 Introduction

The purpose of this thesis is to examine the biopolitics of the credit card industry in its governance over the consumer population through consumer-citizenship, and the manufacturing of consumers into valuable information commodities. Consumer-citizenship is exercised through rights, responsibilities, and performative acts (Isin & Nielson, 2008: 2, 18; Rygiel, 2010: 30; Rose, 1999: 241). The adoption of biometrics and the generation of transactional data trails illustrate the duties and responsibilities of citizenship, as it ensures the rights to security and access (Gates, 2010: 419, 428, 429). Citizenship is integral to the role of biopolitics as it facilitates the management of the population through the exercise of freedom and choice of the consumer (Rygiel, 2010: 36). It is through the entrepreneurship of the citizen-consumer that invokes neoliberal governing 'at a distance' (Rose, 2000: 234), which regulates the behaviour of subjects by appealing to their interests without challenging their autonomous nature (Foucault, 2008: 63-65; Miller & Rose, 2008: 39).'Biometrics as the 'measurement of life' (Ajana, 2013: 3) works through identification and authentication technology by analyzing the "unique characteristics of human bodies, such as fingerprint, iris, voice etc." (Rekola, 2013: 1). For example, fingerprinting and facial recognition verifies transactions (Engagement Bureau, 2016; Harrer, 2016); purchases can be verified through one's heartbeat (MarketWired, 2015) or by snapping a selfie photo (Engagement Bureau, 2016). The employment of biometric technology acts as a biopolitical technique that differentiates the population based on authentication of identity and level of contribution to the economy (Ajana, 2013: 134). While the expansive consumer data trails wrought through

tracking a range of activities produces an informational profile (Gates, 2010: 428; Whitson & Haggerty, 2008: 574) or 'data double' (Haggerty & Ericson, 2000: 606).

This 'securitization of identity,' the binding of data, through the citizenship duties of consumers (Gates, 2010: 420; Rose, 1999: 241) has enabled the credit card industry to identify subjects', monitor financial activity, consumption patterns and connections, and to sort subpopulations into varying categories of risk and value (Gates, 2010: 419, 423, 424). Surveillance technologies not only collect and sort the consumer population but also sell this information (Whitson & Haggerty, 2008: 574; Zwick & Knott, 2009: 224), transforming consumer conduct into 'valuable information commodities', which allows institutions to derive economic value and control the consumer population (Zwick & Knott, 2009: 224). This utilization of consumer data illustrates biopolitical surveillance that capitalizes on making life calculable (Dillon & Lobo-Guerrero, 2008: 268; 282; Foucault, 1978: 143). It is biopower that enables the governance over the population by mobilizing and shaping collective characteristics in order to reach political objectives like wealth and security (Foucault, 1994: 221; Rabinow & Rose, 1994, xi). Individuals as "working, trading, living beings" are integral to these aims (Foucault, 1988: 156). Through consumer-citizenship, biopower is exerted over individuals, enabling the management of life through the constitution and regulation of populations (Rygiel, 2010: 93). As a result, mobility and access to resources are controlled through the sorting of consumers into desirable or undesirable subpopulations, mobilizing freedom for the desirable while limiting it for the undesirable (Ajana, 2013: 125, 133; Byrne, 2007; Foucault, 1978: 142-3; Foucault, 2003: 32-33, 249, 254-5; Foucault, 2007: 11-20; Muller,

2004: 287, 288; Rose, 1999: 243; Rygiel, 2010: 93; van Munster, 2005: 6; Zwick & Knott, 2009: 241).

Research Questions

In light of concerns on the credit card industry's commodification of consumers, I seek to understand how consumers are biopolitically manufactured as consumer-citizens, and are responsibilized in their own production through biometric and transactional data. I analyze Visa and Mastercard Canadian consumer privacy policies, the literature (journal articles, newspaper articles, internet material) on the articulation and connection between the securitization of identity, risk-management, convenient access, and the manufacturing of consumers into marketing commodities through data. I also analyze characteristics associated with consumer awareness or non-awareness on the collection and transmission of consumer data.

This research asks:

1. How do terms and conditions documents convey and operationalize self-responsiblization, particularly the securitization of identity, risk management, and access?
2. What information is collected about consumers and what can be passed to third-parties? Are these parties identified or identifiable?
3. Are consumers made aware of potential risks and effects of their actions?
4. Are there opt-out conditions? When is this permitted and what is the process?

In pursuing these questions, the analysis brings insight into how credit card companies operate within Canada, particularly how personal information is collected, used, stored and disclosed, and how the securitization of identity and the commodification of consumers are enabled. These documents are a means for consumers

to become aware of the conditions they are consenting to, the effects it may have, and potentially take control in limiting the sorting, analysis and distribution of their data double. As a biopolitical apparatus exploiting consumer populations through the dissemination of the data doubles across multiple domains of practice, it is imperative that consumers are aware that they are constituted as information commodities, and how this affects their access to social, economic, and political resources. Furthermore, the analysis on the Canadian Privacy Regime - sections of the Personal Information Protection and Electronic Documents Act (PIPEDA) offers the legal framework on how organizations can act in relation to the utilization of personal information. The analysis examines whether or not the credit card companies meet the legal requirements, as well as if the legislation enables or constrains the exercise of biopolitics within the credit card policy terms.

The literature on the biopolitical dimensions of identity-related developments within the area of surveillance research focuses on managing populations' mobility, access to resources, and security by how they are defined and produced as risks and value through biometric, biographical, and transactional data (Aas, 2006; Ajana, 2013; Amoore, 2006; Boutin, 2016; Cheney-Lippold, 2011; Epstein, 2007; Gates, 2010; Haggerty & Ericson, 2000; Ruppert, 2011; Rygiel, 2010; van der Ploeg 1999a, 1999b, 2003; Wilson, 2006; Whitson & Haggerty, 2008; Zwick & Knott, 2009). This thesis adds to the identity-management literature by examining the credit card industry and the biopolitical strategy involved in the management of consumer populations: The focus of this study is to analyze the literature, and credit card companies 'terms and conditions' on how consumer-citizenship is enabled, and how consumers are manufactured into vectors

of securitization and risk-management. The second aspect concerns how consumers are manufactured into valuable information commodities through consumer data (biometrics and transactional data) and marketed to third parties. A key concern is whether credit card customers are made aware through 'fine print' on the collection and transmission of consumer data. It is argued that it is a biopolitical strategy because consumers are governed through the mobilization of freedom, choice, and self-governance, which subsequently enables their aggregation into subpopulations of value and risk based on the characteristics and behaviour that are seen to drive economic growth.

Firstly, I will outline the shift from disciplinary power to biopolitical power and the differences in techniques of management and constitution of subjects (individuals v. populations) in the move from enclosed surveillance to risk surveillance. Then, I will demonstrate how biopolitics as security is directly connected with the credit card industry's management of the consumer population through consumer-citizenship, with accentuation on the exercise of self-governance, freedom, and choice. The analysis on the securitization of identity will highlight how it is an obligatory and performative act of consumer-citizenship, and how, as a self-responsibilized response to risk and instrument for self-entrepreneurship, it renders the consumer population governable.

Secondly, I will discuss how biometric technologies are a self-identifying tool of privilege that differentiates between included and excluded subpopulations. I will show how credit card companies promote these technologies for consumer security, efficiency, and entitlements, while fostering a biopolitical agenda in which the body and everyday life are subject to modalities of control. I will then discuss the techniques and measures credit card companies' use when quantifying consumer risk. The aim is to show how the

industry defines customers as calculable and predictable ‘codes’ or Deleuzian dividuals while limiting loss and maximizing profit.

Finally, I will illustrate how biometric data in collaboration with transactional data creates subpopulations of risk and value, as a tradable commodity and how the use, dissemination, and manipulation of personal information, exploits subjects through an examination of corporate privacy policies surrounding personal data.

2 Literature Review

2.1 From Discipline to Biopower

Foucault states that power over life began to emerge in the 17th century (Foucault, 1995: 139). The first form of power is an "anatomo-politic of the human body," a disclipinary power that focused on the individual human body, and its correction through confinement, "centered on the body as a machine: its disciplining, … its usefulness and its docility" (Ibid: 139). The second form of power represented a bio-power directed at governing populations for its production and regulation, "a bio-politics of the population" it "focused on the species body, the body imbued with the mechanics of life and serving as the basis of the biological processes: propagation, births and mortality (Ibid: 139). Disciplinary power emerged in 18th century Europe within many institutions or 'enclosures,' from the school to prisons, mental hospitals, and monasteries (Foucault, 1995: 25, 138, 248-9). Disciplinary techniques exercised normalizing techniques through spaces, gazes, and hierarchies. Subjects were highly individualized; strategically they were easier to manage if separated through various dividing strategies (Feeley & Simon, 1992: 450; Foucault, 1995: 167; 248; Lynch, 1998: 840). The purpose was to reform individuals considered disruptive to communities (unruly children, prisoners, mentally unstable) constitutive norms through segregation and rehabilitation (Feely & Simon, 1992: 470; Foucault, 1995: 231, 317; Lynch, 1998: 840).

Through enclosure, a 'political anatomy' was born, one which involved the calculated manipulation and control of the body and its behaviour through hierarchical observation, normalizing judgement, and examination (Foucault, 1995: 138; Rygiel, 2010: 33). Individuals learned to govern and discipline themselves, and to participate in

the production of attitudes, actions and desires that were deemed societally appropriate, such as acquiring the 'taste for work' (Foucault, 1995: 163-169, 239, 240, 243, 248). The panopticon (Foucault, 1995: 248-9) was the political architecture utilized in prison and other social institutions, it had a functional and effective design that ensured every cell in the building was viewable at all times. It individualized, isolated, and normalized through a continual surveillance and cellular separation while diminishing the defiant powers of individuals and simultaneously maximizing knowledge, security, observation, docility, and social and economic utility (Rose, 1999: 187; Foucault, 1995: 167; 208-209, 239, 249-52). This was perceived as the most effective method for controlling and managing deviations to ensure public safety and elimination of crime (Foucault, 1978: 144; 1995: 182-187, 231, 239; 2003: 253; Rose, 1999: 187).

Biopower has a different set of security practices and techniques than disciplinary power. "Bio" originates from the Greek vocabulary, which has two different words for life: Zoe refers to bare life, and bios signifies qualified life or life in a particular form (Esposito 2008: 15). In the latter form, it is a power over life whose inclination is to make life live, to "foster life or disallow it to the point of death" (Foucault, 1978: 138). Biopower manages controls, and intervenes at the level of life in order to increase its vitality (Dillon & Lobo-Guerrero, 2008: 266; Foucault, 1978: 143). These processes transform elements of human life by utilizing knowledge and power to facilitate an apparatus/dispositive (Kristensen, 2013: 11, 16, 19, 44). An apparatus consists of "discourses, institutions, architectural forms, regulatory decisions, laws, administrative measures, scientific statements, philosophical, moral, and philanthropic propositions," a strategic function that responds to a need (Foucault, 1980: 194). The foundation of

biopolitics is contingent on objectives that seek to rationalize phenomenon distinctive to populations (Foucault, 1982: 779-784; 2000: 409-410). Elements of life become subjected to negotiation, management, regulation and manipulation (Rygiel, 2010: 35). Whereas disciplinary power framed the danger posed by the plague for example, through practices of confinement, biopower addresses it through modulated and targeted strategies that map the incidence of contingent behaviour and link it with an assortment of environmental and biological aspects (Dillon & Lobo-Guerrero, 2008: 277; Foucault, 2007: 1-2).

The construction of subpopulations developed in the 18th century through innovative practices of accounting and statistics, depicting patterns of behaviour relating to death, life expectancy, fertility, reproduction, longevity, demographics, wealth, resources etc. (Dillon & Lobo-Guerrero, 2008: 273; Foucault, 1978: 139, 148; Hacking, 1990; 256; Kristensen, 2013: 16; Rygiel, 2010: 93). The creation of these statistical systems were ignited by both civil and commercial and juridical or military-logistical enterprises, as they generated valuable effects i.e. thwarting depopulation, cultivating a growing tax base, and delivering a steady supply of manpower for the military (Hacking, 1990: 256; Kelly, N.D). Populations were rendered more productive and amendable to the maximization of potentialities and minimization of negatives for health, longevity and economic growth (Foucault, 1978: 142-3; Foucault, 2007: 11-20). These techniques, according to Foucault, were not representative either of the legal code or of disciplinary power. "The law prohibits and discipline prescribes" but the function of security is to respond to elements of reality by limiting, checking, and regulating it (Foucault, 2007: 47). The 'regularization' of biopower manages fluctuations within the population (Rygiel,

2010: 102). Foucault labelled this 'dispositif du sécurité; there is no biopolitics that is not inherently a security apparatus (Dillon & Lobo-Guerrero, 2008: 266, 283; Foucault, 2007: Lecture 1, 2). In other words, biopolitics always consists of securitization (Rygiel, 2010: 102).

Security interprets particular phenomena as a natural truth, in which specific points require modification through techniques. Apparatuses of security facilitate a regulatory and promotive function within the population in order for the phenomenon to be cancelled or managed, ensuring favourable effects and an optimization of life (Foucault, 2003: 246; Foucault, 2007: 59). In the pursuit of economic profit, biopolitical industries capitalize on life by managing the "contingent economy of species life" (Dillon & Lobo-Guerrero, 2008: 282) by analyzing the flows of information that present probabilities and patterns of behaviour, correlations and distributions (Dillon & Lobo-Guerrero, 2008; 267-268, Hardt & Negri 2004: 427). This circulation enables industries to monitor and translate "contingency into risk, and risk into a tradable asset" (Dillon & Lobo-Guerrero, 2008: 268). The amalgamation of behaviour and economy is fundamental in mapping out the "correlations of contingent behaviour" to determine the "cost of behaviour" (Foucault, 2007: 1-2). The noncompliant, risky, 'enemy,' or 'excluded populations' may be coerced into compliancy or punished (Dillon & Lobo-Guerrero, 2008: 291; Foucault, 2003: 254). For example, from an insurer's perspective a population is measured as a risk pool, a cost-benefit analysis is used to devise a band-width of acceptable performance and when the cost associated with a loan surpasses the cost of risky behaviour (Hardt & Negri, 2004: 427; Dillon & Lobo-Guerrero, 2008: 278). Lemke (2011) states that Rudolf Kjellén was one of the first to suggest that the state is a "natural

creature;" social struggles, or tensions of life, surface from different interests of classes and groups (Lemke, 2011: 10). Furthermore, social hierarchies exist and are justifiable due to particular facets of evolutionary history (Lemke, 2011: 18-19). Inequalities are inevitable as they represent the difference between those who are self-responsiblized in choice and freedom and those who are not (Ericson, Barry & Doyle, 2000: 533).

Biopolitical security apparatuses govern through the production of freedom, appealing to the interests of subjects for free exchange within the market (Foucault, 2008: 63-65). This facilitates responsiblized self-governance, self-entrepreneurship and regulation of subjects' contingencies of risk and elements of freedom (Dillon & Lobo-Guerrero, 2008: 280-281; 291-292; Foucault, 2007). Freedom enforces the enactment of security, where the management and surveillance over the species-body enables the extraction of vital signs for the advancement, potentiality, and exploitation of life's prospective (Dillon & Lobo-Guerrero, 2008; 273, 291; Foucault, 2007: 310). For instance, the effective regulation of laissez-faire[1] affects a population by generating profit (Dillon & Lobo-Guerrero, 2008: 280; Foucault, 2007: 21, 59; Kristensen, 2013: 61). The notion of laissez-faire states that, in order for there to be beneficial effects to a given population, people must have the ability to participate in the naturalness intrinsic within the population, i.e. to freely exchange within commerce (Dillon & Lobo-Guerrero, 2008: 280; Foucault, 2007: 350; Kristensen, 2013: 61). The rationalization of laissez-faire is justified through empirical techniques of collecting data; this permits an efficient way of enabling the production of knowledge of populations, and for managing fluctuations

[1] Laissez-faire is a political-economic principle in which government should not intervene relating to market and free trade (Merriam-Webster, 2017).
[2] "the study of human control functions and of mechanical and electronic systems

associated with natural phenomena (Foucault 2007: 59). Through both positive and negative means, biopower acts upon populations "as a sort of technical-political object of management and government" (Foucault, 2007: 70). The positive is connected to the strengthening of beneficial effects concurring with the principle of laissez-faire i.e. endorsing health through medicine and increasing profit through the activity of the population within the market. The negative is to decrease risks that are linked to these regularities, for example lessening the mortality rate associated with a given phenomenon through apparatuses of security (Ibid: 70-74; Kristensen, 2013: 62). Therefore, biopolitics in relation to security will proceed to limit risk by acting on the population to support positive phenomena (Kristensen, 2013: 62).

In relation to the credit card industry, the concept of bio-power draws attention to how the consumer-citizen is identified and sorted. Power produces circumstances for knowledge to be obtained and enables how subjects are constituted as members of a population (Foucault, 1995: 194). Knowledge is extracted through a continual assessment of the contingent properties of people's lives using technological devices of surveillance and security, i.e. (biometrics, tracking and screening of transactional data), to determine which subpopulations exhibit preferred lifestyles capable of self-regulation. Different subpopulations demonstrate varying competences in their lives towards self-improvement. Some behaviour, and subsequently some subpopulations are less competent, less valid, or resistant to responsiblized self-governance (Dillon & Lobo-Guerrero, 2008: 291; Foucault, 1997: 297). Techniques of power unveil these hierarchies. Through observable constants, some subjects are identified and produced as superior with surplus value, others are rendered inferior and excluded, limited with access to activities

(Foucault, 2003: 32-33; Rygiel, 2010: 38). This totalizing power that determines the constitution of subjects is justifiable in that it increases the chance of an objective or goal being met for the function of the whole i.e. economic growth (Foucault, 2003: 32-33; 254-6).

The concept of bio-power is fundamental to consumer-citizenship; it is both constraining and productive as it necessitates the management of the population through the exercise of freedom and choice of the consumer (Rygiel, 2010: 36). Foucault (1994) states that a relationship of power is defined not by its direct action on others, but instead by its exercise upon the actions of individuals (137). Power can only be exerted on subjects that are free; "slavery is not a power relationship when a man is in chains, only when he has some possible mobility, even a chance of escape" (139). This means "freedom is a prerequisite for the exercise of power" (Rygiel, 2010: 36). Consumer-citizens can be perceived as free, because they are recognized as having human agency, the capacity to act, and choice in their behaviour and conduct (Ibid: 36). Capitalist principles of access and entitlement are ingrained within consumer-citizenship; it ignites the abilities of free individuals by commending practices of marketization and technologisation (Ajana, 2013: 121, 122). Credit card companies exert power over subjects by appealing to consumer interests for convenience and security i.e. financial transactions through security apparatuses like biometrics (Engagement Bureau, 2016; MarketWired, 2015; PYMNT, 2017). Securitization as a component of biopolitics regulates difference and hierarchy wherein particular facets of life are enhanced enabling the population to be more effectively governed (Rygiel, 2010: 102). Biometric technologies emerge as a security apparatus that governs the entire population (Ajana,

2013: 113; Rygiel, 2010: 102). The implementation of biopower within circuits of consumption encourages consumers to regulate and protect identity by actualizing their 'savoir-faire' (capacity for appropriate action) and optimising their 'savoir-être' (know how) (Ajana, 2013: 118). Yet by placing the onus on consumers to mitigate risk, it capitalizes on neoliberalist ethos of self-autonomy, choice, and freedom (Ajana, 2013: 117, 118; Miller & Rose, 2008: 92). The credit card industry then collects and monitors data on patterns of behaviour and activity of the consumer population, enabling the production of knowledge and management of fluctuations involved with risk and security for the accumulation of economic growth (Gates, 2010: 419).

2.2 Securitization of Identity

The credit card industry exercises biopower by managing consumer populations through identity, and risk-management, with the securitization of identity being one of its fundamental mechanisms (Ajana, 2013: 108; 113). The securitization of identity enables the industry to observe consumer behaviour and control access to financial systems (Gates, 2010: 419). It involves processes and technologies that bind financial, transactional data, and other distinguishing data to subjects through space and time as they cross throughout networks, participate in exchanges with various organizations, and gather assets and debts (Gates, 2010: 420, 424). Rose (1999) states "securitization of identity as the proliferation of sites where individuals are made responsible for establishing their official identity as a condition of access to the rights and responsibilities of (consumer) citizenship" (p. 241). Citizenship practices are always performative in action; subjects constitute themselves as citizens through acts (Isin & Nielson, 2008: 2, 18; Rygiel, 2010: 30). Practices include employment, consumption, and financial transactions in particular, all which demand the authentication of identity (Rose, 1999: 241). For example, you need verification of "who you are to open bank accounts, obtain credit cards, finance, loans and mortgages, to obtain goods or services, or to claim benefits" (CIFAS, 2007). Muller (2004) states that securitization implements citizenship; biometrics as an apparatus either restricts or advances particular rights, entitlements, resources and spaces (p. 279, 288). In other words, it is a performative act, a duty of citizenship to securitize identity, an actualization of 'savoir-faire' and 'savoir-être'. Treating the body as a 'password' discriminates between 'qualified and disqualified bodies', enabling the management of populations, or 'identity management' (Muller,

2004: 280, 287, 288; Woodward, Orlans & Higgins, 2003: 198). This securitization process can be viewed as a "biopolitical maintenance or regulation of the welfare of (consumer) citizens" (Muller, 2004: 285). It appeases security concerns of the financial institution and the consumer, (Ibid: 287) ensuring confidence for the consumer, and generating capital for the industry (Gates, 2010: 429; Muller, 2004: 287).

Since the 1980s, retail banking and credit card industries constructed an extensive network infrastructure and directed a significant amount of focus in developing techniques of automatically identifying and tracking subjects that accessed that network (Gates, 2010: 419). As a result of this process, "identity" became defined as a "disembodied aggregate of transaction-generated data", a "digital representation" of the subject generated over instances and space through the continuous gathering of data (Ibid: 419). It entails particular characteristics and behaviour that describes the profile of the individual, not 'who' is this person, but 'are you authorized' and 'what' kind of a person is this in terms of their fit within a particular subpopulation (Caplan & Torpey, 2001: 3; Butler, 2005: 31; Muller, 2004: 287). Due to the dispersal of data, innovative technologies, conceptions of risk and demand to control mobility, transactions and access to entitlements (Ajana, 2013: 113), identity became recognized as a valuable commodity that requires securitization, a process whereby an identity is contained, a group formed and protected, by both industry and individual efforts (Ajana, 2013: 79, 116, 117, 118; Gates, 2010: 419). The concept of identity fraud and theft in particular is a common risk that faces the interests of the population, and the securitization of identity through biometrics and various other tactics responds as a rationale to this occurrence (Ajana, 2013: 114). Thus, it is integral to understand how the problematisation of identity fraud

functions as a means of mobilizing the "citizen, the consumer" to be "self-managed, self-governed and self-responsiblized" (Ibid: 114).

Identity theft can be perceived as a phenomenon in which biopower acts upon through a positive and negative manner to concur with principle of laissez-faire and limit risk (see above) (Foucault, 2007: 70-74; Kristensen, 2013: 62). For example, economic growth and potentialities are maximized through the activity of consumer populations within the market (Gates, 2010: 418; Whitson & Haggerty, 2008: 574). Furthermore, by verifying identity, the personal and organizational risks associated with identity theft are decreased (Ajana, 2013: 118-119; Gates, 2010: 419; Muller, 2004: 280; Whitson & Haggerty, 2008: 574). Identity fraud is positioned as a systemic risk resulting from the "productiveness of the market" – a methodical byproduct of an innovative, technologically "enabled credit system" (Marron, 2008: 23). Yet, identity fraud impedes upon the principle of laissez faire for beneficial effects (see Dillon & Lobo-Guerrero, 2008: 280; Foucault, 2007: 350; Kristensen, 2013: 61), the ability of a consumer citizen to exercise self-entrepreneurship and freedom within consumerism activities (Marron, 2008: 24). The access to someone's personal data, the stealing of ones identity (Ajana, 2013: 114), the tampering of one's credit ratings, and the affect on 'consumer identity' threatens the ability to consume, and subsequently, limits the ability to govern and establish a life (Ajana, 2013: 117; Marron, 2008: 23-5). In this light, the financial industry shifts the onus onto the consumer to become culpable of risk by adopting self-management, and risk-managing activities (Ajana, 2013: 117; Gates, 2010: 419, 427; Marron, 2008: 34). The industry partakes in 'risk shifting', in which responsibility of risk falls on the individual; 'blameworthiness' is reinforced onto the individual in case of a

'failure' or 'noncompliance' with procedures (McDermott, Henne & Hayes, 2017: 2). Procedures and rules function to facilitate the management of risk and maintain successful organizations (McDermott, et al. 2017: 3). Furthermore, administrative practices and knowledge ensures the public ascertains the perception of risk, and positions the appropriate resources (Salter, 2008: 253). As Whitson & Haggerty (2008) state citizens are encouraged and induced to bring elements of their disembodied data double into securitizing methods of regulation and examination (Whitson & Haggerty, 2008: 574). In this light, identity theft, (a failure) would be blamed on the consumer because they did not comply with the risk managing rules of citizenship. In other words, through risk, individuals are directed in their conduct, which enables the production, ordering, management and controlling of populations (Rygiel, 2010: 67).

These individual efforts are positioned around a neoliberal rationale of risk - 'prudentialism,' in which risk is interpreted as shared, yet is individually acted upon through the calculation and minimization of risk by a citizen (Ajana, 2013: 114, 117; Aradau & van Munster, 2007: 103; Rygiel, 2010: 67). Securitized identities are asserted based on the construction of 'existential' and 'potential' risks (Ajana, 2013: 111, 112; Williams, 2003: 520). In other words, the securitization of identity through biometrics technology manages a whole population through an individualized response to the collective of risks confronting identity (Ajana, 2013: 113). Rose (1999: 239) refers to this mode of self-governance as an "individualization of security," and Whitson and Haggerty (2008: 574) refer to it as "care of the virtual self." A subject who is rational becomes "skilled and knowledgeable about risk" (Rose, 2000: 328). As their own financial managers, identity securitizers are to monitor interest rates (Gates, 2010: 425) and credit

card account statements, purchase identity theft insurance, and contact creditors if errors are suspected (Whitson & Haggerty, 2008: 578). Ajana (2013) notes how financial institutions like Citibank, Barclays, Lloyds TSB and Capital One foster consumers as managers of identity theft risks through advertising, protective services, and online security tips. Varying services allow consumers to monitor credit activities and to receive information on security (116). The same logic advises the adoption of biometric technologies for the securitization of identity, as the credit card industry positions the technology as an essential measure for consumer security and benefit, and a necessary tool for daily financial transactions (Gates, 2010: 427). As Muller (2004) states, the increasingly preoccupation with identity theft or identity fraud has a significant relation between the 'securitization of citizenship' and 'identity management' (287). He goes on to discuss how the financial industry emphasizes the securitization of identity through tactics of 'threat and insecurity.' For example, "Citibank's high-profile advertisement campaign is exemplary in 'securitizing private identity' through both textual/speech acts, and image rhetoric. With fictional episodes involving large-scale fraudulent credit card use, Citibank ads reinforce (or introduce) the need to 'secure' private identity in everyday consumer transactions" (Ibid: 287). The prominence laid on authentication and authorization by financial institutions has initiated the use of biometrics as a securitization apparatus, and "technology of subjectivity" (Ajana, 2013: 118), which has assisted in the production of the hybrid "consumer-citizen" (Muller 2004: 287).

Securitization is then an integral piece that underlines the triad of "biometrics, identity, and citizenship" (Ajana, 2013: 108). Nikolas Rose (2000: 324) concept of neoliberal governing "at a distance" through intervening "technologies of freedom,"

illustrates the credit card industry's governance over the population through consumer citizen self-governance. Under neoliberalism, "to govern better, the state must govern less; to optimize the economy, one must govern through the entrepreneurship of autonomous actors. Once responsibilized and entrepreneuralized, they would govern themselves within a state-secured framework of law and order" (Rose (1999: 139). This form of governance seeks to amend the behaviour of subjects, without challenging their autonomous nature (Miller & Rose, 2008: 39). By the same logic, the credit card industry shapes the activity of consumer-citizens by mobilizing self-entrepreneurship and self-responsibilization without shattering their autonomy and freedom. This is achieved by emphasizing the securitization of identity through biometrics, based on the obligation to view oneself as free within neoliberal citizenship and behaving in accordance with its principles (Ajana, 2013: 114, 126, 127). It is a performative response, an adherence to the requests of "biotechno-scientific capitalist society" (Bhandar, 2004: 273), and an exercise of freedom that 'keeps up' with technological advances, and management of activities (Ajana, 2013: 126, 127). Securitization as a technique of the self coincides with the concept of neo-liberal homo œconomicus and human capital. The foundation of competition-based governance is when populations that consist of active economic subjects engage in the techniques of the self (Foucault, 2007: 183-185; 2008: 145, 282-285). A "citizen-consumer" acts in accordance with "market principles" and continually engages in transactions to "maximise benefits and secure self-interests" (Ajana, 2013: 135). Capital is not only an investment, accumulation, or exchange but an attachment to the entrepreneur, as he is responsible for constituting that capital and security through individual action (Dilts 2011: 136; Foucault, 2003: 224).

Foucault's interpretation of Becker's definition of homo œconomicus is: "the person who accepts reality or who responds systemically to modifications in the variables of the environment, appears precisely as someone manageable, someone who responds systematically to systematic modifications artificially introduced into the environment. Homo œconomicus is someone who is eminently governable" (Foucault, 2008: 270). While Foucault (1995: 222) also states that the management and the manipulation of the population involves techniques that direct people to be active subjects that exercise their freedom in accordance with their own interests (Kristensen, 2013: 51). Based on this logic, the securitization of identity through biometric technology is a response to the environment of the industry. The articulation of it as a means of security and privilege mobilizes the consumer as a free and governable subject. It is an obligation to conduct and view oneself as free, corresponding with principles of choice and autonomy, thus it is also an obligation to utilize biometric technologies as an exercise of freedom (Ajana, 2013: 129). Biometrics then framed around 'rationalisation' is perceived as a reasonable response as it permits for access and convenience, yet, this form of rationality seems to elicit 'inevitably' instead of choice (Ajana, 2013: 127); alluding to the coexistence of control with freedom (Foucault, 2008: 67-8). "Control, in this context is less about the coercive exercise of power and more about the seductive promise of additional freedom, privileged rights and flexible mobility. It is control in the name of freedom itself" (Ajana, 2013: 126). Freedom then is an act of doing, a relational obligation that enables subjectification (Rose, 1999: 94). Simultaneously, freedom through (the securitization of identity) endorses apparatuses of control by instantiating citizenship claims to "movement, access, consumption and entrepreneurial lifestyles" (Ajana, 2013: 127). It

enables a double function that connects “citizens and institutions and citizens and themselves” (Ibid: 127). It operates through the technology of the self, mobilizing freedom to ensure economic and security facilitation while also operating as a tool of governance (Foucault, 2008: 270).

2.3 Biometrics as a Security Apparatus and Technique of the Self

Biometric technologies collect information from the level of the body (Rygiel, 2010: 115). It exercises a biopolitical exchange, in which the 'biological body', or a measure of it, becomes the 'authenticator' (Muller, 2004: 287). Through authentication, identity is verified, while a separate mechanism authorizes identity for entitlement and access (Muller 2004: 286; Woodward et al., 2003: 3). Aas (2006) states that biometrics presents "a binary universe of acceptance or denial, positive or negative, right or false" (151). This excludes any chance of negotiation or doubt, as the 'body does not lie' but tells the truth (Aas, 2006: 151, 153). It makes it a fact that the person is the person he or she claims to be (Rygiel, 2010: 54). Biometric technologies function by automatically connecting bodies with identities, disperses biological and behavioural data across electronic databases, and ensures an accurate and reliable means of verifying identity and authenticating processes (Ajana, 2013: 3). It equates to what Foucault has mentioned as the "progressive animalization of man through extremely refined techniques" (Agamben, 2004: 169). In other words, since the body itself is 'coded' and acts as a 'password' (Aas, 2006: 143) and a 'power relation' (Ibid: 153) manifests as populations become subject to modalities of control and management (Agamben, 2004: 169; Beer, 2014).

Ajana (2013) states, "individual identification cannot be separated from that of 'individual identity'" (26). Similarly, "identification as an individual is scarcely thinkable without categories of collective identity" (Caplan & Torpey, 2001: 3). This illustrates an interwoven relationship between 'individual identification', 'collective membership' and (consumer) citizenship obligations (Ajana, 2013: 26). Membership comprises of a subpopulation that is marked as belonging to a group; individuals are either identified

collectively by inclusion or by exclusion. Citizenship encompasses the assertion of membership, and with it, its rights and freedoms and duties (Ibid: 120, 129).
It is defined as "active and individualistic, rather than passive and dependent" and the economic role of a consumer is integral to the membership of a citizen (Miller & Rose, 2008: 48, 49). Citizenship is exhibited in a subject through the utilization of techniques that assist in achieving 'personal fulfilment' and 'self-advancement' (Miller & Rose, 2008: 48, 82). Consumers are constituted as 'entrepreneurs of themselves' that pursue the maximization of their 'quality of life' through techniques of consumer choice (Ibid: 49). In light of this relationship between the consumer and citizen, biometric technology can be perceived as a technique of entrepreneurship and personal fulfilment that manifests as a duty of citizenship, and practice of membership. The adoption of the technology is a method of self-governance by its 'self-identifying' process; it mobilizes individuals to perceive their action to voluntarily verify their identity and membership as an exercise of choice, instead of direct governance by others (Rygiel, 2010: 132). Biometric technology appeals through its "parasitic vitality" (Agar, 2001: 119) and consumers will implement it into their lifestyle because of its promise of value. By self-identifying, the subject is recompensed with rights and privileges (Rygiel, 2010: 133). Through citizenship the constitution of identity is enabled, which facilitates the conduct of the population toward particular ways and means of governance (Ibid: 31).

The function of biometric technology biologises the consumer-citizen as a homo-oeconomicus - an economic actor; it interconnects neoliberalism and biology while determining identities within a biopolitical scope of governance (Ajana, 2013: 135). The homo-oeconomicus will attempt to 'produce' and 'maximize' his own fulfillment through

diverse methods and 'technologies of the self' (Ibid: 135). Foucault says to be an 'ethical subject' one must engage in techniques of the self, monitoring oneself not only in relation to future investments, but exercising one self in relation to rules of behaviour (Dilts, 2011: 144). Correspondingly, as a citizen who performs according to obligations, a "man of enterprise and production" (Foucault, 2008: 271) will voluntary utilize biometrics for the promotion of economic freedom, and mobility (Ajana, 2013: 135). Banks, and credit card companies position biometric technologies to better address customer needs by enhancing more secure and convenient financial transactions (Engagement Bureau, 2016; MarketWired, 2015; PYMNT, 2017). For example, Visa's "Future of Security Roadmap" highlights the use of biometrics for securing payments in Australia from 2017 to 2020 (Burt, 2017). The approach focuses on four pillars: "devalue data by removing sensitive payment data from the ecosystem and making stolen account details useless; protect data by implementing safeguards to protect personal data as well as account details; harness data by identifying potential fraud before it occurs and increase confidence in approving good transactions and empower everyone, including accountholders and merchants, to play an active role in securing payments" (Visa's Future of Security Roadmap, 2017). "Mobile-initiated payments are ideal for incorporating a wide range of biometrics (e.g. voice, face, fingerprint, iris), given the ubiquity of smartphones and the ease of implementation for both in-store and in-app payments. The promise of eliminating passwords in exchange for a more convenient biometric solution addresses a universal problem shared by nearly all consumers" (Ibid, 2017: 7). Visa checkout, an online payment service (available in many countries including Canada) uses biometrics like Apple Touch ID for purchases (Salisbury, 2015; Visa Checkout Terms and Service,

2018). This fingerprinting recognition grants consumers convenient access to make debit or credit card purchases online, in apps, and in stores from their phone with fingerprint verification in 2013 (Apple Inc, 2017; Dureval, 2017; Violino, 2015).

Nymi™, in collaboration with TD Bank Group (TD), Royal Bank and MasterCard®, established a wearable credit card that verifies purchases through one's heartbeat (MarketWired, 2015). Successful pilots were conducted in 2015 and 2016; several other banks in Canada were expected to launch similar pilots (MarketWired, 2015). Bank of Montreal, Canada's fourth largest lender, in partnership with MasterCard is the first bank to offer a biometric corporate card program - Identity Check Mobile™ in Canada and the United States. This allows customers to verify transactions using facial recognition and fingerprint when accessing online purchases (Engagement Bureau, 2016; Harrer, 2016). BMO customers utilize the program with an app that notifies the consumer when an online purchase requires verification, either by "swiping a fingerprint or snapping a selfie photo" (Engagement Bureau, 2016). This biometric program reduces the need for passwords, or makes the body a password, making digital purchases quick and secure (Ibid). Fujitsu, a multinational information and technology equipment company created an authentication process within ATMs; the customer simply places his palm on a device that scans the veins, which gives access to the account without any physical card (Fujitsu, 2012). Furthermore, Rory Pennington, Senior Analyst at Mapa Research states that biometrics has the potential to extend beyond basic financial functions as logging into a secure banking site, or conducting financial transactions. Since the technology records and digitizes the consumers' identity, this allows for more complex services such as taking out a loan, obtaining insurance, or account onboarding

(Dureval, 2017). This requires banks to prioritize consumer relations; firm level auditing and reporting has mandated attention to "know your customer" (KYC) (Cognizant, 2013, 1). Some banks in Europe have progressed in this area, where to facilitate new-to-bank onboarding processes video identification technology has been employed. The online bank Fidor, in partnership with IDnow (identification and electronic signature solutions), allows customers to on-board via video chat with display of their passport (Dureval, 2017). Fujitsu has implemented biometric technologies for financial institutions to collect, analyze and authenticate documents and the identity of new applicants in less than five minutes (Dureval, 2017). The acceptance of biometric technology then is a necessary duty and act of consumer-citizenship to engage within circuits of consumption, an integral process that identifies members of a subpopulation for the functioning of the market, and an essential measure to maximize an optimal self-entrepreneurial lifestyle.

Consumers have come to recognize the technologies not only as a requirement within consumerism, but now desire to utilize the technology for the purposes of ensuring freedom, and security. Dennis Gamiello, vice-president of identity solutions at MasterCard stated that the introduction of biometrics with Apple and other digital players helped train consumers in accepting the use of biometrics for financial services (Posadzki, 2016). A post-soft-launch survey of BMO biometric program customers discovered that: "Three of every four (74 percent) of participants strongly agree that biometrics are easier to use than passwords. Nine out of ten participants anticipate using biometrics for online payment security in the future" (Engagement Bureau, 2016). According to research conducted by Visa Europe on 14,000 European customers, two thirds of the population surveyed preferred biometrics when engaging in transactions

(Dureval, 2017). Furthermore, amongst the eighteen to twenty-nine age group, almost a quarter stated the possibility in changing banks if biometrics was not accessible to verify money transfers (Dureval, 2017). Another Visa survey on 1,000 Canadians states that 57 percent of consumers perceive biometrics as faster and 65 percent say easier than passwords, 44 per cent state they are more secure than passwords or PINs and 86 per cent are interested in using biometrics to verify identity or to make payments. Canadian consumers are most likely to say they would trust their bank (67%) and their credit/debit card network (51%) to store biometric data, about half of consumers indicate that they would switch away from a card network, bank, or mobile phone provider that does not offer biometric authentication in the future (Visa, 2018). A report by Acuity Market Intelligence predicts that biometrics will drive a global market of 2.5 billion users with 4.8 billion biometric devices by 2020, with revenue of 13.8 billion in 2015. Although biometric technologies initially progressed with governmental entities, it was expected that consumer and enterprise segments would become the dominant portion of the market by late 2017 (Violino, 2015).

These examples illustrate how the growth of the credit card market and transaction infrastructure has initiated the marketing of biometrics as an efficient exercise of freedom, convenient apparatus for consumerism, and consumer protection technology (Gates, 2010: 424; MarketWired, 2015; PYMNT, 2017; Rekola, 2013: 31). With numbers of credit card theft and fraud increasing, the notion to protect one's data double with biometric technologies appears to be a rational choice, and crucial tool for individual security (Gates, 2010: 424, 427). Since biometric technology is comprised of unique bodily and behavioural characteristics it is difficult to duplicate or fake. The risk of

becoming a victim of identity theft, fraud or unwanted financial activity is increased without it and individuals are not assured the security, or even the convenience of never forgetting a password without biometrics (Dureval, 2017; Rekola, 2013: 31, 35; Violino, 2015). In comparison to PINs, usernames and passwords, biometrics actually identifies the customer, since it distinguishes the subject based on biological traits (Rekola, 2013: 31). This may make consumers more inclined to use biometrics as it allows access based "on what they are, not what they know" (Ibid: 31). An individual who submits one's body to the service of the technology to limit uncertainty and risk will also lower industry work volumes, and costs related to "credit card personalization, delivery, management, helpdesk and reissuance" (Rekola, 2013: 32), contributing to labour savings and economic growth (Violino, 2015). Although protection is provided by these technologies, the consumer population's preference for and acceptance of biometrics predominantly operates for the neoliberalist agenda of consumer credit and financial services industry (Gates, 2010: 427).

The institutionalization of biometrics became an apparatus for the finance industry to verify and track financial identities. It served the industry's demand to identify, measure, and categorize the population based on its financial competences and levels of credit risk (Gates, 2010: 419). In the 1980s and 1990s biometrics was implemented by banks to control access for employees, and for "verifying the identity of banking customers using automated systems" (Gates, 2010: 421). Fingerprinting technology was adopted from law enforcement for criminal identification, and businesses manufacturing these technologies began to market toward access control for banking employees, along with customer verification procedures (Ibid: 421). In 1986, a company

called Identix Inc. presented the IDX-50, a smart card fitted with fingerprint technology, as a "useful for access-control applications," and for "verification of credit or debit cards" (Ibid: 421). The finance industry emphasized the need to securitize identity due to the developing industry infrastructures and practices. Innovative systems of identification were required to better authenticate cardholder identity. For example, the "traditional scene of a loyal bank customer being greeted familiarly by a bank teller or branch officer carries more than a message of good relations…. it is also a bank's most secure method of retail customer identification: direct person-to-person recognition" (Trigaux, 1982: 29). Yet a "depersonalization" materialized within modern financial institutions, the 'neighborhood' concept of customer verification no longer applied due to automation, expansion and convenience (Gates, 2010: 422; Trigaux, 1982: 29). As Josh Lauer (2008) states, the credit reporting industry began in the United States in the 1840s "to facilitate safe business relationships in a world increasingly inhabited by strangers," and one of the most significant effects of the formation of credit reporting was the creation of the "disembodied financial identity" (p. 302). This intervention at the level of life creates the disembodied financial identity, enabling biopower in its management over the population (Dillon & Lobo-Guerrero, 2008: 266; Foucault, 1978: 143).

The development of biometric identification was not used to correct a new issue involving security, nor was it solely for improving identification systems to meet the demands of technological and economic progressions (Gates, 2010: 422). Instead, the issue in "monitoring and controlling disembodied financial identities" became more complex along with several interrelated processes (Ibid: 422). These comprised of a reorganization of financial processes around computer networks, and electronic accounts,

and the initiative to make the Internet a profit-making apparatus. Furthermore, the expansion of the credit card industry and equivalency in sorting consumers into subpopulations of risk and value (Ibid: 422, 424). This growth of the credit card industry generated substantial amounts of transactional data, and the increase in credit card use and growing transactional infrastructure significantly increased the issue in verifying cardholder identity. "Whereas paying cash never required an identity check (unless there were restrictions on the product or service being purchased), credit card transactions were obviously more problematic because cards could easily be lost or stolen or obtained in other fraudulent ways" (Ibid: 423). Sociologist James Rule (1973) on his examination of the banking system in the 1970s concluded the verification of subject identity for the authorization of financial transactions was limited without the fingerprint, increasing the risk of credit card fraud (p. 265). In the mid-1980s credit card fraud grew substantially, costing the industry millions of dollars per year. Credit card companies like MasterCard began considering the use of biometrics (fingerprinting) in credit card transactions, as well as the eventual replacement of the plastic card with some type of electronic bodily identification (Ibid: 423). The future goal would be to incorporate bodies directly into the financial network of transactions (Ibid: 423). This convergence of the body with technology is what formulates citizenship practices that enact identity management, it actualizes biopower through the obtainment, sorting and sharing of biometric data (Ajana, 2013: 134; Muller, 2004; 201).

These examples illustrate how biometrics development and wide spread deployment is used as an apparatus of biopower with which to govern everyday financial conduct (Gates, 2010: 419; Huysmans, 2006: 97). These identification systems

implement the function of classification in that specific subpopulations are 'marked' holders of 'a surplus of rights' (Balibar, 2002: 83). As Muller (2004) states, biometrics is an act of citizenship that authenticates identity for "access to rights, bodies, spaces and so forth" (280). It allows for the exercise of privilege, and authorization of access (Aas, 2006: 150). Biometrics then can be perceived as an act of freedom that epitomizes citizenship, since it enables financial mobility and self-maximizing choices (Ong, 2006: 501) that coincide with neoliberalism values of autonomy, governance, and entrepreneurship (Miller & Rose, 2008: 48). As Isin (2004, 220) states the "formation of a subject…is not simply an object of or subject to governmental projects but is governed through its freedom." Freedom allows access, yet it is also continually assessed for conduct that is a threat to the "autonomous exercise of freedom and mobility" (van Munster, 2005: 5). Based on this logic, the technology provides the ability to divide the population into subgroups, designating others more desirable than others (Rygiel, 2010: 49). In fact, it has the power to reject certain subpopulations (Byrne, 2007). Those, who refuse to engage in biometrics are categorised as risky, (Rygiel 2010: 132, 133) thus they potentially renounce their responsibilities as citizen-consumers and can be excluded from access to resources (Ajana, 2013: 129). For example, financial processes, including access to online banking or more complex financial operations may be denied, transactions may not be feasible with cash, cheque, or with the use of a credit card alone without biometric integration (Gates, 2010: 425; Dureval, 2017). Inequality, as a result of choice, materializes through groups of inclusion and exclusion; there are no rights or entitlements without individual responsibilities (Ericson et al., 2000: 555). This inadequate exercise of freedom equates the subpopulation as undesirable, a threat that

requires containment. The objective then is to enable freedom for the desirable citizen population (Ajana, 2013: 129; Foucault, 1978: 256; Rygiel, 2010: 103).

Foucault states citizenship as an apparatus of biopolitics enhances the life of desirable populations (Rygiel, 2010: 100). Thus, the biopolitical relationship between biometrics and the consumer-citizen enhances the life of individuals as members of the desirable population. Yet, this relationship enables the 'calibration of the individual body to the species body – requirements of the economy' (Isin, 2004: 221). Calibration brings consumer life into the "realm of calculation," (Rygiel, 2010: 113) in other words the adoption of biometrics not only produces a productive population and enhances the life of the consumer-citizen, but also functions for the whole economic condition of the credit card industry. In other words, biometrics, although a technique of the self, is "integrated into structures of coercion or domination" (Foucault, 1993: 23). Through a technique of domination one "has to take into account the points where the technologies of domination of individuals over one another have recourse to processes by which the individual acts upon himself" (Ibid: 23). These two techniques in collaboration exert how individuals, are governed by others, by governing themselves (Ibid: 23). Since biometrics effectively governs at a distance, institutions are able to remain far removed from the choices of others, yet maintain a governing position (Aas, 2006: 152) by managing the movement and constitution of populations (Ericson, et al., 2000: 533; Rygiel, 2010: 119). This translates to the gathering and storage of personal information into databases (Rygiel, 2010: 124), monitoring and controlling consumers' access to transactional systems and financial activity, and sorting subpopulations according to levels of value and risk (Ajana, 2013: 134; Gates, 2010: 423, 424, 428). This extraction of knowledge constitutes

populations as more governable through the division of the population (Rygiel, 2010: 124). The widening of the gap between the desirable and undesirable subpopulations allows the former group to facilitate growth of capital while optimizing quality of life; while the latter is classified into forms of exclusion (Foucault, 1978: 142-3; Foucault, 2003: 32-33; 254-5; Foucault, 2007: 11-20; Rygiel, 2010: 105, 124; van Munster, 2005: 6).

2.4 Risk Categorization, Choice, and the Responsibilization of the Consumer

The development of biometric technology along with computerized informational networks allow for the increasingly automation of data collection and analysis for the purposes of calculating the economic value and risk of consumer subpopulations (Ajana, 2013: 165; Zwick and Knott, 2009: 234, 235). Marketization and consumerization has created a "disembodied mass of financial data" (Gates, 2010: 429) from everyday flows, transactions and activities, which pervade risk. This has increased the use of techniques of evaluation, the continuous monitoring and cost-benefit analyses that identify threats, and reduce and neutralize them (Dillon & Lobo-Guerrero, 2008: 268; Rose, 1999: 240; Rose, 2000: 324). The 1950s and 1960s birthed an innovation of mass consumer credit, broadening the scope and potentialities of consumer choice and consumption. The credit card industry adopted a new way of "managing consumers as a population rather than as individual subjects" (Marron, 2007: 108). Statisticians and consultants commissioned technologies like statistical credit scoring to determine creditworthiness; it calculates the measure of productiveness and identification of risk of the consumer-citizen (Marron, 2007: 104, 110; Miller & Rose, 2008: 37). This statistical expertise became applied for the purposes of understanding and acting upon consumer populations as risks (Marron, 2007: 124). Lenders were given a new means of governing consumers, the control of financial movement through the use of an objective, scientific, and empirical scoring model that established norms of risk against which the consumer population would be measured (Ibid: 104).

This type of intervention was sanctioned under legislation as a way of ensuring equal opportunity within the market, based on a subject's competence for self-

government (Marron, 2007: 104) - corresponding with neoliberalist concepts of laissez-faire and homo œconomicus. Access to circuits of consumption and financial conduct is made conditional as certain points need to be passed in order for individuals to access the benefits of regulated financial freedom and liberty (Rose, 1999: 243). "Rights and benefits are contingent upon individual market performance" (Ong, 2006: 500) "and by fixing identity in terms of biological characteristics" (Ajana, 2013: 135). In other words, self-governance is implemented through the infusion of capitalism and biology (via biometrics) under biopolitical governance (Ibid: 135). This infuses prudency in those who wish to achieve this level of freedom through the active calculation of their conduct, which simultaneously refines the standards for inclusion, and produces varying forms of exclusion (Rose, 1999: 243; Rose, 2000: 324, 327). Balibar (2004) states "every institution of citizenship involves the institutionalization of exclusions, following different modalities" (76, 68). Surveillance automizes data through technologies like biometrics and computer databases (Lyon, 2003a, chap 3). These technologies are used because of risks and the inclination to manage populations (Lyon, 1993, 20). Risk-profiling techniques corresponding with biometrics technologies construct classifications of exclusions (Rygiel, 2010: 120). The purpose is to more effectively manage populations because of the individualization of risk that emerged with the rise of neoliberalism, and the requirement to "continuously calibrate the individual self-identities with institutional ones" (Rygiel, 2010: 119). Credit is then based on the financial identity of the consumer and the individualized choices that affect accountability, performance, and risk-management (Lauer, 2008: 305). This is determined through the behaviour, probabilities, and the calculated competency and culpability of the consumer and those in a similar

"risk pool" (Dillon & Lobo-Guerrero, 2008: 267; Marron, 2007: 124). For example, private insurance firms are refining their standards of risk amongst their customer population; this ensures self-responsibilization of the customer and excludes the costly (Ericson, et al., 2000: 555). Exclusion has two divisions, namely, those who are categorized as risky yet are still incorporated through a "principle of activity" (Rose, 1999: 240) and those who are "anti-citizens" (Ibid: 240), that is, the subpopulation that is rejected from circuits of credit consumption due to their incompetence to defend against risks (Marron, 2007: 124-125). All groups are responsibilized in a sense; the excluded however exercise their irresponsibility through a choice and action of freedom that results in failure - the responsibility of the risky (van Munster, 2005: 6). Yet the risky are able to "re-attach to circuits of civility" through rational, self-governing behaviour (Rose, 1999: 240). In other words, those defined as risky but still incorporated are not excluded from all markets, resources, avenues etc. They are still able to engage in circuits of consumption, however their categorization of risk, their level of responsibilization, depicts the level of freedom in consumerism. Marron (2007) states "they are thus made responsible for their own capacity as consumers, for the consuming costs and horizons of opportunity implicit in their individualized projects of consumption" (124). Also, as Rose (1999) states "conditional access to circuits of consumption and civility", is based on the "constant scrutiny of the rights of individuals to access certain kinds of flows of consumption goods" (243). There are no rights or entitlements without individual responsibilities (Ericson et al., 2000: 555), thus, certain goods, credit etc. are dependent on inclusion or level of exclusion, which is determined through the continuous monitoring of the individuals' capacity and action of responsibilization. In this sense,

management over the population is flexible (Rygiel, 2010: 66); because it allows and controls for circulations and movement to take place, and shifts between the good and the bad (Foucault, 2007: 66).

It is through (consumer) citizenship that biopolitics constructs the included from the excluded; as subjects are responsible in understanding the distinction between high and low risk behaviours and resulting consequences (Rygiel, 2010: 28, 67). Risk pricing is based on the creditworthiness of the consumer, the probability of consumer non-payment on a loan, and if the cost associated with the availability of credit surpasses the cost of risky behaviour (Dillon & Lobo-Guerrero, 2008: 268, Marron, 2007: 103-104). For example, variables like "income, property, education and employment" dictate a subject's capacity and probability of non-payment (Marron, 2007: 112). Thus, 'deserving' consumers pay less while 'underserving' consumers' pay more (Makuch 2001: 16). Subjects who were previously excluded for their attribution of risk may 're-attach', although with higher credit card interest rates, while subjects with low-risk are offered more credit at a lowered cost, ensuring compensation "for the differential costs of default presented by differential categories of risk" (Marron, 2007: 122). This enables the potentiality for more consumption, and ultimately market growth (Edelberg 2003: 20-1; Johnson 1992: 28; Liñares-Zegarra and Wilson, 2012: 2, 5; White, 2004: 503-4). The emphasis on prudentialism for the regulation of risk is a mechanism of biopower. It implicates the whole consumer population to pragmatically calculate risk within individual behaviour, as risk is calculable only when spread throughout a population (Ewald, 1991: 203; Reith, 2004: 395). To ascertain risk, a probabilistic analysis measures known factors in the past (recursiveness of events), to determine future contingencies of

default. A level of certainty and predictability based on consistencies and patterns is integrated into more complex assumptions of risk for defining the profitability of a consumer (Liñares-Zegarra and Wilson, 2012: 5; Marron, 2007: 104, 110, 118, 121; Reith, 2004: 395). Different types of risk scoring enable different measures to identify risk; risk-based pricing consists of the FICO credit score; unpaid credit card debt (short-term and outstanding) (Liñares-Zegarra and Wilson, 2012: 3). The FICO credit score changed the aspect of risk from analyzing only discontinuous variables within a confined population of a creditor's customer inventory into analyzing standardized, continuous measures of risk compared with the national customer population (Marron, 2007: 117). Application scoring determines acceptance or rejection, along with the type of conditions/interest rate administered. Behavioural scoring continually monitors the performance of the subject in order to determine the renewal of a credit card account, credit limits, and targeted marketing (Marron, 2007: 117; Ong, 2006: 500). Risk pricing, as an overall process can be perceived as a biopolitical tool of governance. It functions through regularization; it manages fluctuations by rendering the population amenable for economic growth (Foucault, 1978: 142-3; Foucault, 2007: 11- 20, 47). Profit is the objective, and its probability is conceived upon the self-governance of the consumer population, as they are held accountable for their consuming costs and optimization of opportunities (Marron, 2007: 124). Conceivability of a future threat is within the confines of human action; the subject is autonomous in the construction of their own trajectory and stabilization of outcomes by recognizing and responding to the mediation of risks (Reith 2004: 396). In other words, this process individualizes responsibility for the potentiality

to consume (Marron, 2007: 111); it organizes and produces subpopulations in risk hierarchies, which ultimately limits or expands consuming capabilities (Reith, 2004: 385

This continuous regulative control over subpopulations can be represented through modulation (Rose, 2000: 325), as Deleuze states, through coded language individuals are not created, but endlessly sub-divisible "dividuals" through the gathering of personal data depicting recursiveness of events and choices (Deleuze, 1992: 5). They are not subjects with an inherently fixed character, but with competences and potentialities that are transformed into codes, profiles, security ratings etc. Subjects are a coded assortment of information based on "credentials, activities, and qualifications for entry into this or that network" (Rose, 1999: 234; Rose, 2000: 325). It is not a mechanism that seeks to socialize or discipline subjects under the panopticised surveillance of a permanent individualized gaze. Instead this represents a form of biopolitical surveillance, in which activity is monitored through the flows imbedded within everyday life and restructured by logics innate within networks (Ibid: 234; Ibid: 325). This production of the dividual, the multiplication of 'data subjects' (or data doubles), the risk score and profit probability, signifies a cybernetic[2] relationship between consumers and biopolitical networks. Information machines continuously collect data to identify, and discriminate individuals into categorized subpopulation profiles (Elmer, 2004:41). Enacting a type of control and governance that seeks to regulate behaviour across the population to ensure maximum efficiency and minimization of the negative as a whole (Feeley & Simon, 1992: 452; Foucault, 2007: 70-74; Rose, 1999: 234; Rose, 2000: 325). Biopolitics is

[2] "the study of human control functions and of mechanical and electronic systems designed to replace them, involving the application of statistical mechanics to communication engineering" (Dictionary.com, n.d).

focused in achieving this state of balance through controlling random occurrences by predicting the plausibility, or compensate for the effects of it (Foucault, 2003: 249) Deleuze states control (e.g. of risk, as in the case with credit card companies) occurs within internal processes of digital networks, it is analyzed and managed not through "static media and fixed architectures, but by 'codes'" (Zwick & Knott, 2009: 235). Codes are flexible in nature and function, they identify and simulate in ways that fixed enclosures cannot (Bogard, 2007). They also can be reconfigured to revise assessments of value, risk, and adjust access (Zwick & Knott, 2009: 235). For example, Guattari's (in Deleuze, 1992: 7) explanation of control, "one would be able to leave one's apartment, one's street, one's neighborhood, thanks to one's (dividual) electronic card that raises a given barrier; but the card could just as easily be rejected on a given day or between certain hours; what counts is not the barrier but the computer that tracks each person's position – licit or illicit – and effects a universal modulation". Thereby, the continuous extraction and measurement of consumer data bits into new formations of risk that determine profitability is a modular effect that breaks down life, and conceptualizes it as a code (Zwick & Knott, 2009: 235, 236). It is precisely biopower that enables this governance over the population by mobilizing characteristics that render the consumer-citizen visible and knowable in order to attain particular objectives (Marron, 2007: 119; Foucault, 1994: 221; Rabinow & Rose, 1994, xi).

2.5 The Biopolitical Manufacturing of the Consumer through Biometrics and the Data Double

Foucault (2003) states that biopower emerges when it becomes technologically feasible for man to manage life, particularly with surveillance apparatuses and tactics of human control. This can be illustrated through Haggerty & Ericson's term of the 'surveillant assemblage,' it operates by extracting bodies from territorial spaces, and recoding consumer activity into distinct flows and virtual data doubles which can be analyzed and targeted for intervention (Haggerty & Ericson, 2000: 606). Negroponte (1995) states that 'being digital' is the alteration of the physical, into electronically produced bits and bytes. These digital traces of our life become an economic advantage when they not only are identified, but also analyzed, sorted and distributed (Dodge & Kitchen, 2005: 855; Zwick & Knott, 2009: 228). Biometrics is meant to authenticate identification by matching data with a specific person (Cavoukian, 1999: 3). Biometric technology is "an identifier": "it does not define a person's identity or who they are, rather it links specific data with that person" (ibid). If biometrics only verified identification of a person through the measurement of the body, then it would not be a biopolitical tool (van der Ploeg, 1999b: 40), yet as a biopolitical tool, it provides a 'raw' instantaneous truth extracted from the body, which is processed into a 'refined' truth for specific political objectives (Aas, 2006: 154; Ajana, 2013: 91-92, 102; Ruppert, 2011: 226).

This refined truth or knowledge is the breakdown of everyday activities into bits of information (dividual), for purposes of management and profit (Dodge & Kitchin, 2005: 857; Haggerty & Ericson, 2000: 619). Transactional data tracks the movement,

behaviour and performance of subpopulations and biometrics binds this data to the subject by verifying and authenticating identity (Ruppert, 2011: 221). These surveillance practices fall under the pretext that they are for the biopolitical well-being of the population; they are 'efficient and technologically neutral,' yet they operate to "camouflage" the discriminatory politics they enable (Hunt & Rygiel, 2006; Rygiel, 2010: 129). Instead of removing partiality, biometric, risk profiling and data mining technologies reduce the discriminatory process as more "technical and scientific" (Rygiel, 2010: 129). In other words, the utilization of codes i.e. fingerprints, characteristics, profiles, credit score, etc (Aas, 2006: 155; Rose, 1999: 234) involved in these technologies is not neutral (Curry, 2004; Lyon, 2003a, 2003b; Rygiel, 2010: 129). The quick, routine monitoring, updating and analyses of codes, and their ability to provide authentication to grant access enable the power to discriminate (Dodge & Kitchin, 2005: 855). This renders the population governable by 'social sorting' through 'digital discrimination', which subsequently affects the life-chances of individuals (Curry, 2004; Lyon, 2003a, 2003b; Rygiel, 2010: 129). Together, these bio-technological techniques of surveillance conceptualize Deleuze and Guattari's (1992) 'double assemblage,' as their harmony derives from the fact that they function unanimously (Patton, 1994: 158; Huysmans, 2006: 97). Biometric technology is actualised in the 'machinic' assemblage as it enables the identification of subpopulations and allows for interconnected databases of credit card and marketing companies (Bogard, 2006: 105). It is the material and data that facilitate the distributions of the data double and flows of information entailing consumption and production across networks (Bogard, 2006: 105; Zwick & Knott, 2009: 229). The 'enunciative' assemblage is where risk, claims and truth

statements are defined and produced, in so that varying levels of value are attached to the data double (Bogard, 2006: 105). Essentially, the consumer population has been transformed into a digital assemblage, an assemblage, in which a subpopulation exists and obtains meaning (Zwick & Knott, 2009: 229). In other words, biometric technologies transform human identity into patterns of information that produce new formations of identity (Aas, 2006: 144). The process is an 'informatization of the body,' in which flows of information translated into digital codes alter the identity of the person and its conceptualization (Rygiel, 2010: 145; van der Ploeg, 2003: 24, 58, 64)

Biometrics and transactional data has the potential to violate privacy measures as it directly affects one's ability to decide and control the use of their data (Alterman, 2003: 145; Ruppert, 2011: 219). Privacy is a "claim of individuals, groups or institutions to determine when, how and to what extent information about them is communicated to others" (Westin, 1967: 7). Security and privacy issues related to the storage of biometric data along with other identifying data is a concern (Rekola, 2013: 33), particularly that financial companies are objectivizing, merging and sharing personal information with disparate, disembedded systems and databases (Marron, 2008: 24). Haggerty & Ericson (2000) state that the surveillant assemblage transforms the institution of privacy by surpassing institutional boundaries when its intent to "serve one purpose finds other uses" (p. 606, 616). 'Function creep' refers to technology being used beyond its intended purposes (European Commission, 2005: 16) when, for example, the functional purpose of biometric technology leads to the manipulation of its system and exploits the capabilities of data mining [3] (Ajana, 2013: 47). Another similar term is 'knowledge discovery,' this

[3] The analysis of peoples behaviour to establish profiles (Dodge & Kitchin, 2005: 876)

occurs when data mining techniques discover new aggregate knowledge, often independent of the subject's consent. Individuals may not even be aware that this data exists, or that it is being used, analyzed, manipulated, and sold (Office of the Privacy Commissioner of Canada, 2014). The objective of knowledge discovery is to unveil patterns from people's behaviour, when used within financial services it "affects the life chances of millions in terms of credit scoring", and it also is used to "channel particular goods, services, information, opportunities, and life chances to some people and not others" (Dodge & Kitchen, 2005: 876). What is stored about an individual is "constitutive and inseparable from who that person is" (Ajana, 2013: 14), and with respect to van der Ploeg (2003) this calls for an imperative reconsideration of the effects of invasive forms of monitoring, classifying, and analysing and effectively 'controlling and manipulating' populations through the interventions on the body and generation of identities (70-1). Alterman (2003) states this bodily 'representation' throughout systems and databases causes privacy loss and damages the self-respect of individuals (143). In accordance with Kant's ultimate moral principle - one should treat humanity only as ends in themselves, never as a means (Kant, Schneewind, Baron & Kagan, 2002) - Alterman (2003) positions that the utilization of a person's body as a means to an end is analogous in obliging that person to surrender his body and with it, his 'free will' (p. 145).

Through the activity of a subject (biometrics and transactional data) (Ruppert, 2011: 227) a 'metaphysical piece of yourself' is surrendered (Alterman, 2003: 143). In other words, the actions of subjects permit for the 'enactment of population objects' (Ruppert, 2011: 227), it grants others to use your identifying data for their own objectives, and potential misuse of data, which makes it difficult to maintain control over

(Alterman, 2003: 143, 144, 145), challenge, or intercede in the production and circulation of their data double (Ruppert, 2011: 227). Furthermore, the threat to privacy and security is greater with biometrics since it is stable, offers greater certainty than other identifying data alone, and cannot be changed (Alterman, 2003: 145, 146; Rekola, 2013: 50). As Boutin states, in relation to the collection and sharing of information, "it is practically impossible for anyone to find all the information being passed around about themselves, or to correct it" (2016). The circulation of the data double through a multitude of differing 'centres of calculation' operate for services and power that are generally unknown to the subject (Haggerty & Ericson, 2000: 613). This loss of control, and objectification of the body and determinability of identity through these identifying technologies creates a sense of 'alienation' from one's body (Alterman, 2003: 146). The identifying process does not merely uncover subjects as already shaped and fixed, but instead it 'produces' their identities and particular abilities (Ruppert, 2011: 224). As Foucault (1983) states, "a subject is not to be subjected (connoting disciplinary power) but to be subjectified" (Ruppert, 2011: 224). In other words, data subjects are produced through other actors that determine their identity and classification (Ruppert, 2011: 224). Furthermore, this classification of the data subject is constructed and projected with a measure of value, alluding to Muniesa, Milo & Callon's (2007) 'economic agencement', it is the process whereby 'things, behaviours and processes' are rendered 'economic' (3). As Dodge & Kitchen (2005) state, this economic identity, that they refer to as 'capta shadow' is produced through the behaviours and transactions of individuals, and have become 'valuable, tradable commodities' as demonstrated by the growth of "credit

reference agencies, lifestyle profiles, and geodemographic systems[4]"; yet individuals lack the ability to control the constitution of it, or its use (Dodge & Kitchen, 2005: 859). Essentially, the acceptance of biometric technology and engaging in the production of the data double renders the consumer population transparent, and subjectified, with limited power; it enables credit card companies to exercise biopower by acquiring control of consumers' bodies, and tracking and differentiating the population as measurable commodities.

Biopolitics is drawn to a cybernetic conception, associated with multiplicative practices involving the "formation, coding, de-coding, and algorithms," of networks of data (Dillon & Reid, 2001: 65). Information resulting from flows of the surveillant assemblage is constructed for "governance, commerce and control" (Haggerty & Ericson, 2000: 613). Subjects invoke copious amounts of identity markers through the body's movements and locations. Successions and patterns enable the accumulation of data towards a particular configuration of a person (Ajana, 2013: 19, 134; Whitson & Haggerty, 2008: 574). Once a subject is identified, this unit can be acted upon, processed in a manner that clusters them with other similar units to suit particular purposes (Coll, 2013: 204; Dodge & Kitchin, 2004: 853). Essentially, the power to monitor and define nearly all consumption and non-consumption behaviours of consumers facilitates the production of consumer identities (Zwick & Knott, 2009: 227). Identity, produced through codes by mathematical algorithms occurs in data-processing systems such as banks and marketing companies (Cheney-Lippold, 2011: 165-6; Dodge & Kitchen, 2004: 853, Zwick & Knott, 2009: 234). Billions of transactions are recorded each day, which

[4] "Study of the population and its characteristics, divided according to regions on a geographical basis" (mbskool.com).

produce comprehensive records of times, date and location of transaction (Dodge & Kitchin, 2004: 853). These transactions in themselves are an 'identity check', they document i.e. what a person reads, choice in drink and play, travels, etc. (Gates, 2010: 423; Turow, 1997: 44). They indicate a "person's behaviour, health, consumption activity" (Whitson & Haggerty: 574), and "habits, preferences, and lifestyles" (Haggerty & Ericson, 2000: 611). It unveils clusters of associations amongst "demographic, attitudinal, behavioural, and geographical features of a population" (Turow, 1997: 44). Each access to a privilege creates another entry into a database; a further marker toward the data double that facilitates a constant reproduction, and revision of an individual's score (Haggerty & Ericson, 2000: 611, 613; Rose, 2000: 326; Ruppert, 2011: 223, 226; Whitson & Haggerty, 2008: 574; Zwick and Knott, 2009: 235). The use of the data double is a valuable commodity that enables unlimited social sorting of consumer populations into governable categories of value and risk (Dodge & Kitchen, 2005: 859; Gates, 2010: 423-424; Stalder and Lyon, 2003: 90; Zwick & Knott, 2009: 222, 224). Lyon (2003b, 1) states "surveillance today sorts people into categories, assigning worth or risk, in ways that have real effects on their life chances." Surveillance categorizes populations into groups for inclusion and exclusion (Lyon, 1993, 20) through technologies that automize data, i.e. biometrics and risk profiling (Lyon 2003a, chap 3). These technologies enable a "social sorting" through "digital discrimination" (Rygiel, 2010: 129). Illustrating a biopolitical surveillance that seeks to control and manage subpopulations by 'textualizing' or reducing identities by mere personal details (Lauer, 2008: 301; Lyon, 2003a: 5). The textualization of identities dates back to mercantile agencies in the late 19th century, Lauer (2008) states the system identified, categorized,

predicted and valuated persons as economic subjects for commodification and distribution purposes (p. 304, 323). This imperfect representation of the textualized, enumerated financial identity created consequential affects for the individual, and still remains today (Gates, 2010: 424; Lauer, 2008: 320, 321).

Credit-card firms are selling consumer credit card transactional data to marketing, advertising companies, and data brokers[5], yet they do not inform consumers, for fear of repercussion (Kaye, 2013). These technologies are efficient and cost-effective processes that are not inhibited by obstructions of space and time that are inherent within physical surveillance. They do not require excessive labour, they are inconspicuous, and they are stable (Rose, 2000: 326; Ruppert, 2011: 221). Venture Development Center acts as an intermediary amongst data brokers and brands and data suppliers, the company stated the majority of credit card companies engage in data monetization[6] (Kaye, 2013). The sharing of data-collecting practices between private companies enables governance over populations, controlling mobility and access (Rygiel, 2010: 78). The American Civil Liberties Union (ACLU), an advocacy group for the privacy rights of Americans, describes that a "major factor driving the trend toward data surveillance forward is the commodification of personal information by corporations" (Stanley & Steinhardt, 2003: 4; ACLU, 2004). Private corporations are not accountable to citizens nor do they accurately portray their representation. Therefore, their increasing participation in monitoring the activities of subjects fosters concerns over the issues of responsibility,

[5] "Data brokers are companies that collect personal information about consumers from a variety of public and non-public sources and resell the information to other companies" (The Federal Trade Commission, 2012).
[6] "Data Monetization can be defined as maximizing the revenue potential from available data by institutionalizing the capture, storage, analysis and effective dissemination of that data" (Zimmermann, 2011).

access and possession of data (Rygiel, 2010: 78). In 2011, Mastercard Advisors developed an Information Services sector that approached media-agency trading desks with an appealing offer: data entailing purchases of 80 billion consumers (Kaye, 2013). Mastercard joined Maxpoint, a digital-ad firm that aggregates publicly available data such as health data, to distinguish population characteristics within particular ZIP code regions (Kaye, 2013). Maxpoint then "sells display, mobile and video ads", which contain targeted coupons, or store offers on behalf of CPG – Consumer Packaged Groups, and other forms of advertisers i.e. restaurants (Kaye, 2013). Essentially, a pizza joint may utilize the classification system to push promotions in areas where populations engage in more fast-food transactions (Kaye, 2013). Mastercard also disperses segmented transactional data through Exelate, a data-management company that converts information from Mastercard and other associate companies "including Acxiom and Nielsen into digital-ad exchanges for targeting" (Kaye, 2013; Out-Law, 2011). This targets subpopulations more likely to shop at particular stores (Kaye, 2013). American Express transforms transactional data into income through its Business Insights consulting sector, which has targeted mail and online proposals to consumers on behalf of advertisers on an aggregate level (Kaye, 2013). Visa also sorts consumers into cohorts based on different factors, including purchasing history and location, before selling the data to marketing companies (Out-Law, 2011; Reisinger, 2011). The company has a patented application that uses credit account transaction data to target digital ads. The profile generator even contains non-transactional data i.e. address, online information from social media, google searches, credit bureaus, insurance claims and even DNA databanks (Lowcards.com, 2012). This is a "systematic modulation of the consumer

population," as personal information is continually updated, mined, and distributed (Zwick & Knott, 2009: 223). This makes subpopulations knowable and calculable in relation to a product. It "creates and causes to emerge new objects of knowledge and accumulates new bodies of information;" (Foucault, 1980: 52) producing categorizing practices that generate profiles of limited or expanded access (Dodge & Kitchin, 2005: 878; Cheney-Lippold, 2011: 175; Gates, 2010: 423-424; Haggerty & Ericson, 2000: 613, 615; Rose, 1999: 245; Ruppert, 2011: 221-222).

Lyon (1993, 23) explains, "the assessments and judgements made on data subjects depend on coded criteria, and it is these codes that make surveillance processes work in particular ways." To demonstrate this, Lyon (2003b) states that surveillance technologies are contingent upon classification programs that are constructed around searchable databases. Marketing companies for example, use these classification programs to organize and sort consumer populations into different groups (p. 14). As aforementioned, this coding is not neutral because it exposes deductions and calculations that are made about these populations in a manner that labels them. This process then effects the decisions regarding the offering of products and services to varying populations (Rygiel, 2010: 129). Lyon (2002, 1) denotes this as the "phenetic fix;" used "to capture personal data triggered by human bodies and to use these abstractions to place people in new social classes of income, attributes, habits, preferences, or offences, in order to influence, manage or control them." This discriminatory process is illustrated in the manufacturing process of the consumer score through informational characteristics and narratives. The consumer score, or profile is a computer-generated number that denotes a specific total to a consumer, its perceived economic value for a particular commodity, or toward an area

of consumption (Zwick & Knott, 2009: 233-234). It is similar to FICO credit scores, yet they are not regulated as to what factors may not be used, nor is their regulation in the transparency or accuracy of the score (Boutin, 2016). Like a FICO score, a consumer score ascertains risk and value through probabilities on known factors and may save businesses large costs i.e. save insurers the costs of undercharging a risky client (Boutin, 2016). Although, these scores can negatively affect certain subpopulations, it may affect potential careers, schools, insurance, etc. and potentially create secrete blacklists (Boutin, 2016). Data brokers like Acxiom purchase data from credit card companies and gather more identifying data from other sources. Derived data elements infer certain characteristics of a subject, and patterns of correlations, i.e. location data and purchasing data may reveal race or health status through algorithms (Boutin, 2016; Cheney-Lippold, 2011: 165, 175; Federal Trade Commission, 2014: 19). For example, health insurance may reject to cover for an individual because of their unhealthy food choices indicated by transactions; this infers the subject is obese with increased health issues (Coll, 2013: 211). Information may entail gender, class, race, sexual orientation; illnesses like HIV and depression, or histories of substance abuse, which is then sold to clientele (Boutin, 2016; Cheney-Lippold, 2011: 165). As Curry (2004) states certain narratives state that "people who are in spatial proximity with one another are associated one with another… people do things that are like those done by people with whom they associate" (494). In other words, 'flawed' or undesirable subpopulations are thereby made known and discriminated against through the constraint of options (Lyon, 1994: 154). Giorgio Agamben's (2004) refers to these processes of identification as "biopolitical tatoos," where bodies are marked and grouped as good or bad citizens (p. 169). As a mechanism

of control, these practices of identification regulate the amount of freedom permissible for particular subpopulations (Cheney-Lippold, 2011: 166; Huysmans, 2006: 97). They represent a knowledge constructed on a 'one-way observation,' (Aas, 2006: 153) that enables a regulatory mechanism that intervenes in the embodied existence and lives of persons. Opening or closing possible encounters, i.e. access to circuits of consumption, treatment and benefits, and mobility for varying groups (Ajana, 2013: 75, 92; Dillon & Lobo-Guerrero, 2008: 266; Dillon & Reid, 2001: 48, 57; Dodge & Kitchin, 2005: 853; Haggerty & Ericson, 2000: 618; Rose, 1999: 243; Rose, 2000: 326).

Through biometrics, the body materializes as instantaneous 'truth'. The purpose is not only to obtain information about the identity of subjects, but also to manufacture identities (Aas, 2006: 154). As Van der Ploeg (1999a) states that identifying technologies do not necessarily identify a pre-existing identity, but function as a means of establishing an identity (300). It is a conceptualization of the data double through the "tentacles of the surveillant assemblage", the reduction of the "flesh to pure information' (Haggerty & Ericson, 2000: 613). Many attributes of a score/profile are accurate, although data can be further manipulated, and 'partial' or 'underdetermined' identities are produced for manufacturing purposes and economic value (Boutin, 2016; Zwick & Knott, 2009: 233). Sunil Gupta, analytics expert at Insight, explains the function of the score from the viewpoint of the economics of customer production.

> "For our clients, it's of course important to know who is likely to respond to *their* message and buy *their* products. For them, talking to someone who won't buy their products, no matter what, is a big waste. So, they come to us to tell them which is which by ranking thousands of

> individuals according to a model we prepare for the client. Each individual gets a score and then we provide the client with deciles to make it easier for them to compare the different segments of the market for their specific product. Our database is huge, so we believe we can really parcel out the true scores for each member of the population we look at and the client has a lot of confidence in the targets and non-targets we provide them with" (Zwick & Knott, 2009:233).

This process targets and manufactures consumers as 'valuable information commodities' through the collection, analysis, categorization and sharing/selling of personal information, depicting a modular simulation that controls customers, while creating economic growth (Zwick & Knott, 2009: 224, 238, 239). This assemblage of the population as commodities and potentialities illustrates Foucault's teaching of biopolitics; it is the extraction of life's 'vital signs' to use them for promotion and exploitation (Dillon & Lobo-Guerrero, 2008; 273). As Thacker (2005) states, information in biopolitics is that which is, and produces, the material, the biological and embodiment of "life itself" (p. 28). Here, life becomes dispersed, "weighed and valued", a biopolitical approach that "capitalizes life" by "regulating the contingent economy of species life" (Dillon & Lobo-Guerrero, 2008: 268). Foucault's focus was not in how establishments, governments, and knowledge operate in their own sake, but instead, how they work in relation to the 'making of subjects' (Foucault, 1994: 126-127). This capitalization and commodification process that 'makes up subjects' illustrates how surveillant apparatuses enable a subjectification of the subject, an operation over the population that functions as a 'means to an end'. Rather than being an accurate or inaccurate depiction of subjects, the

surveillant assemblage pragmatically enables institutions to discriminate populations (Haggerty & Ericson, 2000: 614). A 'digital discrimination' implemented through the use of "computer codes, algorithms and narratives" (Rygiel, 2010:132). That segregates consumer subpopulations into functional hierarches, presenting those that exemplify more value from less value for a particular product, marketing message etc. (Zwick & Knott, 2009: 234). An exercise of biopower that renders the consumer population manageable through 'caesuras,' a fragmentation within the whole population that exploits the biological continuum of life (Foucault, 2003: 254-5). In other words, the constructions of categories that make up people (Cheney-Lippold, 2011: 173; Zwick & Knott, 2009: 241), 'loci's of inclusion and exclusion' (Rose, 1999: 243), illustrate a targeted control, and modification of human life; a 'calculated biopolitics' that extracts and maximizes forces from the human body towards the production of a particular form of life (Kristensen, 2013: 20, 26, 38, 65).

3 Data and Methods

Research Design

The research design for this study is document analysis. "Document analysis is a systematic procedure for reviewing or evaluating documents--both printed and electronic (computer-based and Internet-transmitted) material" (Bowen, 2009: 27). Data is to be examined with the intent of extracting "meaning, understanding, and empirical knowledge" (Ibid: 27). Documents analyzed are logged without a researcher's involvement, and consist of text and images (Ibid: 27). Examples of documents may include newspapers, organisational or institutional reports, survey data, books, public records etc. They are referred to as 'social facts' since they are made and distributed in means that are socially ordered (Atkinson & Coffey, 1997: 47; Bowen, 2009: 27). This data can be located in "libraries, newspaper archives, historical society offices, and organisational or institutional files" (Bowen, 2009: 27).

With document analysis, a review of literature is integrated into the study, when previous studies are included raw data is not analysed; only the interpretation of that data is used (Ibid: 27). There are many different functions/use for documentary material (Bowen, 2009: 29). In relation to this study, data in documents can provide additional information to the study, and knowledge base. Or they can be used to validate findings or evidence derived from other sources (Ibid: 30). For example, in a study on teacher education programs the researcher (Hoepfl, 1994) used newspaper reports, university policy documents, and department self-evaluation data in corroboration with interviews (Hoepfl, 1997). The combination of data sources is referred to as triangulation – "the use of multiple methods or data sources in qualitative research to develop a comprehensive

understanding of phenomena" (Carter, Bryant-Lukosius, DiCenso, Blythe and Neville, 2014: 545). There are several different types of triangulation (investigator, theory, data source, method); data source triangulation in particular is significant to this study, as it uses several (at least two) sources of data (Bowen, 2009: 28; Ibid: 545). For example, data source triangulation could consist of public records with a written document (Write.com, 2018). Triangulating data provides credibility since it reduces potential bias by testing the validity (trustworthiness) through the convergence of multiple sources of evidence (Bowen, 2009: 28; Carter et al., 2014: 545; Eisner, 1991: 110).

The analytic process involves "skimming (superficial examination), reading (thorough examination), and interpretation" (Bowen, 2009: 32). This involves finding, choosing, evaluating and synthesising data comprised in documents. Data is extracted from key words, phrases or passages, and then structures and codes them into themes, categories, and key concepts (Labuschagne, 2003: 101). It is an iterative process that uses components of content analysis and thematic analysis. Content analysis organizes information into categories associated with the main research questions (Bowen, 2009: 32). Thematic analysis recognizes patterns and emerging themes within the data that develop into categories for analysis (Fereday & Muir-Cochrane, 2006: 82). The process involves more of a meticulous focus on reading and review of the material. Characteristics within the data are selected for the construction of codes and categories that reveal major themes. Predefined codes may also be used, particularly if the document analysis is supplementary to other sources in the study (Bowen, 2009: 32). Objectivity and sensitivity (reacting to subtle meanings) is to be used when analyzing documents (Ibid: 32).

There are many advantages of document analysis. It is an efficient, less time-consuming method, as it selects data instead of collects data. It is more available, accessed through public domains and the Internet (Bowen, 2009: 31). It is a more cost-effective than other methods, and more likely to be used when it is not viable to collect new data. There is a lack of obtrusiveness and reactivity, and there is stability since documents are not affected by the research process, or researcher. This counters issues of reflexivity innate within other qualitative research methods. Documents remain appropriate for repeated analyses. There is exactness; names, references and details are included (Ibid: 31). Limitations of document analysis include insufficient detail, since some documents may be produced for non-research purposes. There may be low retrievability with some documents, and an inadequate gathering of documents may insinuate 'biased selectivity' (Yin, 1994: 80). Document retrieval from organisations is mainly affiliated with corporate policies that adhere to the organisation's agendas (Bowen, 2009: 31). Furthermore, because the documents in this study are not for research purposes – specifically the credit card companies' terms and conditions, there is only a portion of detail, which does not thoroughly answer the research questions. Thus the concept of biopolitics is not entirely addressed and examined, which limits the theoretical framework of the study. However with document analysis there is enough detail to understand how elements of biopolitics, particularly how consumer-citizenship is indicative in the terms through securitizing identity, responsibilization of risk and consumerism, and commodification of customers from an empirical level, as expressed in the analysis section.

Data Collection

In this study, I combined data sources by analyzing Visa and Mastercard Canadian privacy policies and the literature (journal articles, newspaper articles, internet material). Since the policies are used to verify the literature, a few are suitable in providing sufficient information for the research (Bowen, 2009: 33). The analysis of two sets of policies along with the literature triangulates the data, offering credibility, and reducing potential bias (Bowen, 2009: 28; Carter et al., 2014: 545; Eisner, 1991: 110). The documents are stable and exact, indicating a lack of obtrusiveness and reactivity, countering any issues of reflexivity and suitable for repeated analyses (Bowen, 2009: 31). Although corporate policies are more likely aligned with the organizations principles, and there is the possibility of insufficient detail, the advantages of using document analysis outweigh the limitations. There is no software or additional instrument used other than the human instrument. Using content and thematic analyses complements the research questions as information is organized into categories that relate to the research questions, and patterns and themes are recognized within the policies that develop into categories for analysis (Bowen, 2009: 32; Fereday & Muir-Cochrane, 2006: 82). Furthermore, the Canadian Privacy Regime - sections of the Personal Information Protection and Electronic Documents Act (PIPEDA) is the legislation that informs organizations on the utilization of personal information. The analysis of relevant sections of PIPEDA interprets whether the privacy policies of credit card companies meet the legal requirements or not by comparing the content and words listed. The analysis also examines if the limitations set out in the law enable or constrains the credit card companies' exercise of biopolitics.

Measures

"Theory driven code development" is a common approach in social science research (Boyatzis, 1999: 33). The theory instigates the researcher to formulate indicators or evidence that support the theory, the elements of theory or hypotheses drives the substance of the code (Ibid: 33). Precodes consisting of words and/or phrases are grouped into 5 categories. This predefined framework is used as a data management tool for organizing sections of similar or related text to support in analysis (Crabtree & Miller, 1999). The use of a template offers credibility to the study since it provides a trail for evidence (Fereday & Muir-Cochrane, 2006: 84). The codes are derived from material within the literature and research questions through a theoretical lens of biopolitics. The structure of the codes in this study is partly from Boyatzis (1999, 31) instructions on developing meaningful thematic codes. This consists of "a label, (i.e. a name), a definition of what the theme concerns (i.e., the characteristic or issue constituting the theme), and a description of how to know when the theme occurs (i.e. indicators on how to "flag" the theme)". "A 'good thematic code' is one that captures the qualitative richness of the phenomenon. It is usable in the analysis, interpretation and presentation of the research" (Boyatzis, 1999: 31).

Securitizing identity (larger category) – Definition: As the proliferation of sites where individuals are made responsible for establishing their official identity as a condition of access to the rights and responsibilities of (consumer) citizenship. Descriptive phrases: "collecting information on activities" "personal information you provide us with" "conducting payment transactions" "information/action required for said purposes" "identifying information".

Risk management (subcategory) – Definition: Actively responsibilized in minimizing risk and threats i.e. fraud. Shifting of risk onto individual. Descriptive phrases: “security” “protect” “prevention of illegal activity, threats or violations,” “not responsible for other companies practices” “customer review other policies”.

Convenient access/consumerism (subcategory) – Definition: Entrance into circuits of interests. Descriptive phrases: “personalize experience” “access to features” “fulfill your requests” “marketing” “contests”.

Commodification of consumers – Definition: Production of consumers into tradable assets from data. Descriptive phrases: “collection and sharing of personal information” “aggregation of customer information for said purposes, i.e. marketing” “engagement or transferring of information with third-parties”.

Awareness on the utilization of data - Definition: Explicitly articulates the purpose, collection and sharing of data. Descriptive phrases: “use” “collection” “sharing” “purpose”.

The thematic research analysis, as depicted as a deductive systematic step-by-step procedure using a prior template is also an iterative and reflexive practice (Fereday & Muir-Cochrane, 2006). It is search for recognizing patterns and emerging themes that are integral to the analysis and description of the phenomenon (Daly, Kellehear, & Gliksman, 1997; Fereday & Muir-Cochrane, 2006: 82). The stages of data collection and analysis in this study were conducted simultaneously; this ensures a comprehensive analysis that consists of “careful reading and re-reading of the data” (Rice & Ezzy, 1999: 258). The data is analyzed for its sufficiency in supporting the phenomenon conveyed in the research questions, and lastly translated and presented (Hoepfl, 1997). The primary

objective was to from the data on how biopolitics is conceptualized through the credit card companies' terms in managing the customer population through consumer-citizenship. With specific focus on: securitizing identity, customer responsibilization of risk and convenient access/consumerism, and the commodification of consumers. The thematic coding, and iterative process enables the ability to recognize and decipher the themes and patterns associated with biopolitics, and any indications or implications that make these facets of biopolitics empirical and evident throughout the terms and conditions.

4 Data Analysis

Canadian Privacy Regime and the Limits of Law

The purpose of the Personal Information Protection and Electronic Documents Act, is "… to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances" (Personal Information Protection and Electronic Documents Act, SC 2000. c. 5, s. 3). Sections from the act are analyzed that specifically relate to, and provide a foundation for interpreting the credit card privacy policies legal obligations, and application or non-application of biopolitics and consumer-citizenship. The principle sections are: Accountability, Identifying Purpose, Consent, Limiting Collection, Limiting Use, Disclosure, and Retention, Accuracy, Safeguards, and Individual Access.

Securitization of identity and Convenient Access/Consumerism

Visa and Mastercard privacy policies clearly state the emphasis on the securitization of identity. One phrase in particular articulates this: parties may access cookies, and tracking technologies on your computer or device in order to 'collect information about web-browsing activities…over time and across different websites and services' (VISA Privacy Policy, 2016). This reiterates to how technologies bind distinguishing, transactional data to subjects through space and time as they cross networks, and participate in exchanges with various organizations (Gates, 2010: 420, 424). Furthermore, personal information is used and shared with financial institutions or

merchants to “process payment transactions”, “including authorization, clearing, chargebacks and other related dispute resolution activities” (Mastercard-Global Privacy Notice, 2017). The customer must establish/authenticate their identity (give identifying information) for access to engage in transactions; this translates to subjects constituting themselves as (consumer)-citizens through rights and responsibilities, and performative acts (Isin & Nielson, 2008: 2, 18; Rose, 1999: 241; Rygiel, 2010: 30). Citizenship practices as performative acts (Isin & Nielson, 2008: 2, 18; Rygiel, 2010: 30) consist of engaging in transactions, and consumerism, all which require the authentication of identity (Rose, 1999: 241). Foucault (1995: 222) states the management and the manipulation of the population involves techniques that direct people to be active subjects that exercise their freedom in accordance with their own interests (Kristensen, 2013: 51). Thus, citizen-consumers act in accordance with ‘market principles’ and continually engage in transactions to “maximise benefits and secure self-interests” (Ajana, 2013: 135). Citizenship is significant to how biopower is exercised, because “power can only be exerted over subjects who are free” (Foucault, 1994: 139). Consumers are seen as free citizens because they have the ability to make choices (Rygiel, 2010: 36); instantiating citizenship claims to “movement, access, consumption and entrepreneurial lifestyles” (Ajana, 2013: 127).

The policies significance on attaining personal information for customer consumption and convenient access is further alluded in how Mastercard and Visa monitor data and for what purposes. The companies state their service providers, partners and third parties may collect, and use information about your activities and patterns of behaviour on their websites, pages and apps, and other third-party applications and

websites to administer advertisements and content based on individual interests. Visa calls this practice a 'behavioural advertising practice', or 'retargeting' (VISA Privacy Policy, 2016). Visa and Mastercard state that personal information is used to fulfill requests, respond to inquiries, and manage accounts, along with communicating promotions, services and contests of the company and third parties. For example, personal information is shared "with third parties whose features you use in connection with our products and services, including social networks" (Mastercard Global Privacy Notice, 2018). "If you sign up to receive offers from retail or travel partners through Visa, we may share your Personal Information with those partners as needed to provide promotions and marketing communications, to validate referrals, measure success of such promotions, or operate the programs" (Visa Global Privacy Notice, 2018). In other words, those who securitize identity – the responsibilized homo-oeconomicus – are 'marked' holders of a 'surplus of rights' (Balibar, 2002: 83), the personal information given or obtained "is any information that we can use to identify, locate or contact you" (Visa Global Policy Notice, 2018). Since customers submit personal information either directly or through other third parties, engage in transactions, and consent to tracking technology they pass those required points that need to be met in order to gain access (Rose, 1999: 243). They enable the identification of themselves, the 'marking for rights' through the securitization of identity. A biopolitical process that represents a 'calibration of the individual body to the species body – requirements of the economy' (Isin, 2004: 221) and calibration brings consumer life into the "realm of calculation" (Rygiel, 2010: 113). In other words, securitizing identity not only produces a productive population and enhances the life of the consumer-citizen by offering access to circuits of consumption

and resources, but also functions for the whole economic condition of the credit card industry.

Section 4.3.8 of PIPEDA states*, "an individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal"* (PIPEDA, SC 2000. c. 5, s. 4.3.8). Mastercard and Visa give customers the choice to opt-out of the automated collection and use of certain information, for example, behavioural-targeted advertising and marketing practices, and receiving certain types of cookies (Mastercard-Global Privacy Notice, 2017; Visa Privacy Policy, 2016). Providing an option of exclusion, as expressed through both the credit card terms and enforced by legislation enables the biopolitical governance over a population by segregating those subpopulations considered undesirable; this ensures containment of the undesirable and enables freedom for the desirable citizen population (Ajana, 2013: 129; Foucault, 1978: 256; Rygiel, 2010: 103). The level of exclusion depends on the amount of identifying data permitted and activity engaged in by the consumer. For example, Mastercard states that individuals can simply limit the use of online activity, opt-out of cookies, "refrain from conducting payments or from submitting personal information" to avoid their personal information and identity from being used and shared. However, Mastercard does state that, "there are consequences from failing to do so" (Mastercard-Global Privacy Notice, 2018). Not engaging in consumerism activities and providing personal information is a mechanism of control that restricts access and entitlements, as listed in the terms 'products and services, apps, or online services' may not be accessible, or access to 'certain content and product features' may be denied (Mastercard-Global Privacy Notice, 2017; Visa Privacy

Policy, 2016). This indicates that there are several levels of exclusion, to opt-out of cookies or limit activity online is one level of exclusion, in which the group of customers is still incorporated through a "principle of activity" (Rose, 1999: 240). These customers are still incorporated to consume because they securitize their identity (Rose, 1999: 240), although they are excluded from receiving certain services, and marketing and advertising by both the credit card company and third parties.

To not securitize identity i.e. not provide the personal information requested, nor engage in financial transactions, is another level of exclusion that would fit the concept of an "anti-citizen" (Rose, 1999: 240); this excluded group negates rational, self-governing behaviour of citizens (Rose, 1999: 240). Although the terms and conditions do not specifically state the 'consequences' of not "conducting payment transactions", and not "submitting personal information", it is noted, "there are consequences of failing to do so" (Mastercard Global Privacy Notice, 2018). There are risks and effects of their non-actions, and it can be implied that if a customer does not comply they are denied their right to be citizen-consumer. Deprived of the neoliberalist principle of laissez-faire for free exchange within commerce (Dillon & Lobo-Guerrero, 2008: 280; Foucault, 2007: 350; Kristensen, 2013: 61) and ability to maximize self-interests and benefits (Ajana, 2013: 135). Since citizenship is exhibited in a subject through the utilization of techniques that assist in achieving 'personal fulfilment' and 'self-advancement' (Miller & Rose, 2008: 48, 82), those that fail to pass points for access and benefits negate citizenship, thus are constituted as 'anti-citizens'. These groups essentially create their own inequality, as there are no rights or entitlements without individual responsibilities (Ericson et al., 2000: 555), they are undesirable due to an exercise of irresponsible choice

(van Munster, 2005: 6). In other words, through (consumer) citizenship, biopolitics manages the population, and regulates their freedom by constructing the included from the excluded (Rygiel, 2010: 28, 67). Those who refuse to exercise their duties of consumer-citizenship forfeit the benefits, they are rendered as disqualified bodies because they do not authenticate their identity or act performatively; thereby they are not conducive or productive in relation to the market (Foucault, 2008: 147; Rose, 1999: 241). As Dodge and Kitchen state the analysis of people's behaviour and patterns is used to "channel particular goods, services, information, opportunities, and life chances to some people and not others" (Dodge & Kitchen, 2005: 876). These examples from the credit card policies, and the applicable section of PIPEDA indicate how biopower governs the population through the freedom, choice and responsibility of consumers, particularly how convenient access to circuits of consumption and the optimization of an entrepreneurial lifestyle are enabled for those groups who exercise the duties of consumer-citizenship by securitizing identity, while consequences – or categories of exclusion – are enabled for those that exercise their rights and freedom irresponsibility; contrary to the principles of consumer-citizenship.

Securitization of identity and Risk Management

Biopower in exercised within the policies by using risk management as a component of securitizing identity; this mobilizes the consumer to be self-responsibilized citizens. The company is able to govern better and increase profit by governing less, "through the entrepreneurship of autonomous actors" (Rose: 1999: 139). For example, Visa states that personal information is used and shared to 'analyze and monitor website

usage, secure websites, prevent, investigate and take action against fraud, threats and enforce policies' (VISA Privacy Policy, 2016). Personal information is used to 'protect against unauthorized transactions, claims and other liabilities, and manage risk exposure and security of our payments network' (Mastercard-Global Privacy Notice, 2017). Also, personal information is shared and disclosed to 'prevent fraud, and to ensure security of payments and transactions' (Mastercard-Global Privacy Notice, 2017). Clearly articulated in the policies, securitizing identity allows credit card companies the ability to biopolitically govern the customer population by monitoring customer behaviour and activities, and control and regulate access (Gates, 2010: 419). The terms enable governance through the autonomy and freedom of consumer-citizens by mobilizing customers to consent to the use and sharing of their personal information for their own welfare, and security. It illustrates how credit card industries are able to govern the population 'at a distance' (Rose, 2000: 324), through the choices of the customer. Identity fraud as a risk in particular impedes upon the capability of a consumer citizen to exercise self-entrepreneurship and freedom within consumerism activities (Marron, 2008: 24). By highlighting 'threat and security' the customer population is mobilized to securitize identity, particularly the securitization of everyday transactions (Muller, 2004: 287). Coinciding with Whitson and Haggerty (2008), this logic encourages citizens to bring elements of their disembodied data double into securitizing methods of regulation and examination (574). Thus, customers will consent to the utilization of their personal information to "protect against and prevent fraud, unauthorized transactions… and verify your identity" (Mastercard-Global Privacy Notice, 2018). This securitization process can be viewed as a "biopolitical maintenance or regulation of the welfare of (consumer)

citizens" (Muller, 2004: 285). A biopolitical apparatus that facilitates a regulatory and promotive function within the population, that cancels or manages a phenomenon i.e. fraud, ensuring favourable effects and an optimization of life (Foucault, 2003: 246; Foucault, 2007: 59). It facilitates a type of governance that seeks to amend the behaviour of subjects, without challenging their autonomous nature (Miller & Rose, 2008: 39). In other words, securitizing your identity is a biopolitical apparatus that governs through freedom by appealing to the interests of citizens (Foucault, 2008: 63-65); appeasing the interests of security concerns of the financial institution and the consumer (Ibid: 287), ensures confidence for the consumer, and generates capital for the industry (Gates, 2010: 429; Muller, 2004: 287).

Onus is shifted onto the consumer to become culpable of risk by adopting self-management, and risk-managing activities (Ajana, 2013: 117; Gates, 2010: 419, 427; Marron, 2008: 34). Visa states "we are not responsible for the collection, usage and disclosure policies and practices (including the data security practices) of other organizations, including any personal information you disclose" (VISA Privacy Policy, 2016). Personal information disclosed – consenting to the use of that information ensures the individual bears the risk, not the company. This coincides with 'risk shifting' the responsibility of risk falls on the individual; in the event of failure, 'blameworthiness' is reinforced onto the individual (McDermott, et al., 2017: 2). Visa states "we may share your Personal Information with merchants and other partners through Visa's partnerships, co-branded or promotional programs or websites, but only to the extent you have a relationship with such partner or you authorize the sharing… We may share your Personal Information with other partners, but only if we have your consent". A failure,

for example, could be Visa sharing personal data to a partner that leads to negative consequences to the customer, yet blame is placed on the customer because they consented to its use. As La Porte (2013) states procedures are listed "to assure that responsibility/blame is placed on the workforce, not placed on senior institutional actors" (259). This hinders workers from raising concerns or disputing practices of the companies (McDermott et al., 2017: 4). In context with this analysis, responsibilization through terms indirectly prevents customers from raising concerns about the company's responsibility for customer information and inhibits customers from challenging the credit card's company practices. This represents the subjectification of the subject, a mobilization that works through the freedoms of consumer-citizenship that enables apparatuses of control to govern the population (Ajana, 2013: 127; Rose, 1999: 94).

Section 4.1.3 of PIPEDA states, *"an organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party"* (PIPEDA, SC 2000. c. 5, s. 4.1.3). This section denotes a constraint on the biopolitical self-responsibilization, risk management, and self-entrepreneurship of consumer-citizens. It limits the company's shifting of risk onto the consumer and the neoliberal governing 'at a distance' (Rose, 2000: 234) by holding the company responsible over the utilization of customer personal information. Although the credit card companies comply with this section of legislation, the privacy terms mobilize the customer to be a responsibilized consumer-citizen. Wherein the customer is accountable for how their personal information is used, even though the credit card companies

facilitate the collection and use of customer personal information. Visa states "we have relationships with third party advertising companies that place advertisements on and perform tracking and reporting functions for our website and other websites. Although we do not share any Personal Information with these third-party advertising companies, they may place cookies on your computer when you visit our website or other websites so that they can display targeted advertisements to you. However, this Privacy Notice does not cover the collection methods or use of the information collected by these companies" (Visa Global Privacy Notice, 2018). Visa provides an opportunity for other organizations to collect information on customers, yet forfeits responsibility, and implies the responsibilization and consent of the customer by emphasizing customers' actions on their website – 'when you visit our website'. Furthermore, Mastercard states they "strongly suggest" the customer review the third-party privacy policies they link customers with, as they "are not responsible" (Mastercard Global Privacy Notice, 2018). Mastercard also states that if they transfer or sell a portion of their business/assets they "reserve the right to transfer personal information," yet they will use "reasonable efforts to direct the transferee to use personal information" provided in conjunction with their Global Privacy Notice. Furthermore, the customer is told to contact the entity about the transfer and processing of their personal information (Mastercard-Global Privacy Notice, 2017).

These individual efforts are positioned around a neoliberal rationale of risk - 'prudentialism,' in which risk is interpreted as shared (implicating the whole consumer population – indicating biopower) yet is individually acted upon through the calculation and minimization of risk by a citizen (Ajana, 2013: 114, 117; Aradau & van Munster,

2007: 103; Rygiel, 2010: 67). A mode of self-governance - 'individualization of security' (Rose, 1999: 239), or 'care of the virtual self' (Whitson & Haggerty, 2008: 574), where one is to be rational, skilled and knowledgeable in terms of potential risk (Rose, 2000a: 328). In other words, through citizen-self-governance, credit card companies shift risk onto the customer, capitalizing on the neoliberalist ethos of self-autonomy, choice, and freedom (Ajana, 2013: 117, 118; Miller & Rose, 2008: 92). Companies govern 'at a distance' by mitigating their responsibility over customer personal information, yet maintain governance over the customer population. Not actively being aware of third party practices and policies in the collection, use, and sharing of personal information indicates a failure to act in compliance with citizenship. Through the exercise of irresponsibility through freedom one is rendered blameworthy for the result in failure - 'responsibility of the risky' (van Munster, 2005: 6). The biopolitical governance through freedom ensures subjects have the choice to contribute to their own prosperity, while also contributing to the prosperity of the population, yet this involves an abjection (or blameworthiness) on those that are not self-governing (van Munster, 2005: 6). The self-governing, self-responsibilization of risk facilitated through the terms is a biopolitical tool that enacts a type of control that seeks to regulate behaviour across the population to ensure maximum efficiency and minimization of the negative as a whole (Feeley & Simon, 1992: 452; Foucault, 2007: 70-74; Rose, 1999: 234; Rose, 2000: 325).

Commodification of the Consumer

The mobilizing of the citizen consumer to securitize identity for access to resources, and to manage risk is an exercise of biopower that allows credit card companies to collect, use and share information. The utilization of customer information enables the categorization and commodification of the population based on value. Personal information Visa and Mastercard collect on the customer population may be obtained from 'financial institutions, merchants, other entities connected with transactions and services, and any publicly available channels' (Mastercard-Global Privacy Notice, 2017) along with any 'social media channels, and third parties' (VISA Privacy Policy, 2016). "For example, if you communicate with Visa using Facebook or Twitter, we may receive additional information about you from your profile. We may also obtain information from third party data suppliers who help us enhance our records" (Visa Global Privacy Notice, 2018). "We may collect Personal Information from third party digital wallets and online merchants when you make an online purchase" (Visa Global Privacy Notice, 2018). Digital wallets for example, Apple Pay, may use biometrics through Touch ID (as mentioned above in section 2.3). Although the terms do not explicitly state the use of biometrics, the assumption is that biometric data would be collected because of the use of digital wallets. The terms state that information can include "contact information (such as name, postal or e-mail address, and phone number), business contact information (such as job title, department and name of organization), username and password, payment account information, photographs, articles and comments, mobile device unique identifier, geo-location data, shopping behavior and preferences, language preference, age, date of birth, gender and family status)"

(Mastercard-Global Privacy Notice, 2017). Along with the "payment card number, location of transaction, time and date of transactions, enhanced transaction information, and the amount of transaction…. demographic data about you or your household such as census records that tell us about the average ages or incomes in a certain neighbourhood" (Visa Global Privacy Policy, 2018).

Section 4.9.3 of PIPEDA states, *"in providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual"* (PIPEDA, SC 2000. c. 5, s. 4.5.2). The terms do not specifically name the organizations they share customer information with, which could again imply the responsibilization of the customer to exercise their duty as citizen and determine that for him or herself. Furthermore, the use and sharing of personal information for security and consumerism purposes to financial institutions/entities, third parties, affiliates, service providers, merchants, partners (i.e. retail and travel organizations) illustrates how credit card companies are able to monitor behaviour and define customer characteristics. As mentioned in the above sections, monitoring and analyzing behaviour for prevention of risk and taking action against threats, and ensuring security of financial activity, along with the use of behavioural-targeted advertising, marketing practices, tracking technologies, and cookies demonstrates a biopolitical surveillance that manages the species-body through the extraction of its 'vital signs' (Dillon & Lobo-Guerrero, 2008; 273, 291; Foucault, 2007: 310; Zwick & Knott, 2009:

224). The monitoring and utilization of customer personal information corresponds with Lyon's (2003b, 1) illustration of surveillance, how it functions to "sort people into categories, assigning worth or risk, in ways that have real effects on their life chances." Enabling a 'social sorting' through 'digital discrimination' (Rygiel, 2010: 129). The policies make note on the anonymization and aggregation of personal information when preparing and furnishing aggregated data reports:

> "including, but not limited to, the following: compilations, analyses, analytical and predictive models and rules, and other aggregated reports for the purpose of advising our issuing and acquiring institutions, merchants and other customers and partners regarding past and potential future patterns of spending, fraud, and other insights that may be extracted from this data" (Mastercard-Global Privacy Notice, 2017).

The aggregation of data conceptualizes how biopolitics is associated with techniques that involve algorithms and coding of information (Dillon & Reid, 2001: 65). Since it is biopower that makes the consumer population visible and knowable through the continuous extraction, and measurement of consumer data bits and reconfiguration into specific categorizations of codes (Gates, 2010: 419; Marron, 2007: 119; Zwick & Knott, 2009:235). Ajana (2013) states, what is stored about an individual is "constitutive and inseparable from who that person is" (14). In other words, customer identities are constructed or represented based on the information collected; "data elements" allow the companies to 'identify and locate you' (Visa Global Privacy Notice, 2018). Aggregated data on spending habits, geo-location, demographic data, gender and family status etc. constructs particular populations, which presents a measure of value or risk for a product

or service within the company, as well as for third party entities. This information consists of 'identity markers' that customers make evident through their locations and movements, which entail of successions and patterns that proceed to configure the identity of the individual (Ajana, 2013: 19, 134; Whitson & Haggerty, 2008: 574). When the individual is identified, the individual unit can be acted upon, processed in a manner that clusters them with other similar units to suit particular purposes (Coll, 2013: 204; Dodge & Kitchin, 2004: 853). For example, "Visa enhances Card Transaction Data and uses it to generate anonymized and aggregated consumer spending and marketing reports and other data products that enable companies to improve their marketing efforts. These solutions help companies identify consumers that they can target. For example, a marketing report may show that consumers in one postal code tend to spend more at auto parts stores than consumers in other postal codes. These products also help companies determine the effectiveness of their marketing campaigns" (Visa Global Privacy Notice, 2018). These processes target and enable the manufacturing of consumers as 'valuable information commodities' through the collection, and sharing of personal information, which depict a modular simulation that creates economic growth (Zwick & Knott, 2009: 224, 238, 239). It is biopolitical because elements of behaviour are "weighed and valued", representing a capitalization of life through the regulation of the "contingent economy of species life" (Dillon & Lobo-Guerrero, 2008: 268).

Section 4.5.2 of PIPEDA states *"organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained*

long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods". Section 4.5.3 states, *"personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information"* Section 4.6.3 also states *"personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out",* and section 4.7 notes that *"personal information shall be protected by security safeguards appropriate to the sensitivity of the information"* (PIPEDA, SC 2000. c. 5, s. 4.5.2, s. 4.5.3, s. 4.6.3, s. 4.7). These sections make the company responsible over the protection and use of personal information, not the customer which appears to constrain the principles of biopolitical self-governance, yet section 4.9 states that, *"upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate… Exceptions to the access requirement should be limited and specific. The reasons for denying access should be provided to the individual upon request"* (PIPEDA, SC 2000. c. 5, s. 4.5.2). This section however implies the self-responsibilization of consumer-citizens in governing their own data double as reflected in the credit card privacy terms.

Visa states individuals have the right to access and edit personal information they store, and Mastercard states that customers in "certain jurisdictions…you may have the

right to request access to and receive information about the Personal Information we maintain about you, to update and correct inaccuracies in your Personal Information, to restrict or to object to the processing of your Personal Information, to have the information anonymized or deleted" (Mastercard Global Privacy Notice, 2018). Visa does state, "we use physical, technical, organizational, and administrative safeguards to help protect your Personal Information from unauthorized access or loss. For example, we use technology like encryption to protect sensitive Personal Information (such as your account number) during transmission. We will retain your Personal Information for as long as the information is needed for the purposes listed above and for any additional period that may be required or permitted by law" (Visa Global Privacy Policy, 2018). Mastercard states "we also take measures to delete your Personal Information or keep it in a form that does not permit identifying you when this information is no longer necessary for the purposes for which we process it, unless we are required by law to keep this information for a longer period" and that they comply with "mandatory retention periods provided by law" (Mastercard-Global Privacy Notice, 2018). Although individuals have these options available for correcting data or preventing the utilization of their data, and information is only obtained for a period of time and for purposes listed above and deleted (Visa does not say however that they delete the data, only Mastercard), and safeguards are in place for the protection against unauthorized access or loss. There is still the potential to use and share inaccurate data if customers are not actively being aware and responsibilized on the utilization of their data, and correcting inaccuracies. Furthermore, once data is shared the ability to retrieve personal information that has already been shared/multiplied to third parties is more difficult. As Boutin states "it's

practically impossible for anyone to find all the information being passed around about themselves, or to correct it" (2016). In other words, biopower manages the customer population by responsibilizing the customer to rectify or prevent the use of their data double. Yet, handing over a 'metaphysical piece of yourself' (engaging in transactions) makes it difficult to maintain control over, challenge, or intercede in the production and circulation of a data double (Alterman, 2003: 143-145; Ruppert, 2011: 227). Furthermore, the dissemination of the data double through varying 'centres of calculation' function for services and power that are generally unknown to the subject (Haggerty & Ericson, 2000: 613). This dichotomous relation illustrates how biopower is both constraining and productive (Rygiel, 2010: 36). Power is not directly acted upon customers, but it is exercised upon the actions of the customer (Foucault, 1994: 137). Customers are thereby mobilized to engage as free citizens by presenting personal information, yet power and control is enabled over the customer through their own actions, making it difficult for the customer to retain control over their data double.

This biopolitical concept is further conceptualized in the purposes of customer information. It is difficult to determine if information is utilized for purposes outlined in the terms, function creep may arise, as the initial collection and sharing of data has the potential for it to be used beyond its said purposes (European Commission, 2005: 16). Section 4.2 of PIPEDA states that *"the purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected".* Section 4.2.2 indicates, *"The Limiting Collection principle (Clause 4.4) requires an organization to collect only that information necessary for the purposes that have been identified.* Section 4.3.3 *states "an organization shall not, as a condition of the*

supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes". Furthermore, section 4.2.4 states*, "when personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose".* Section 4.4.2 also states *"the requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception"* (PIPEDA, SC 2000. c. 5, s. 4.2, 4.2.2, 4.3.3, 4.2.4). The credit cards' terms and conditions indicate the purposes of collection and use of personal information that may be obtained, yet Mastercard states (as seen above), that personal information may be used for "other insights", which could imply information being used beyond what is explicitly specified in the terms, which raises concern over the collection of 'necessary information' for said legitimate purposes. Furthermore, they state that personal information may be used to "serve other purposes for which we provide specific notice at the time of collection, and as otherwise authorized or required by law" (Mastercard Global Privacy Notice, 2018), this could imply that the customer is not guaranteed that the purposes for using/sharing personal information will be as listed at the time of consent. Furthermore, when information is shared with third parties, 'purposes' may go beyond what is explicitly stated in the terms. For example, Mastercard and Visa state they share personal information with third party companies, public authorities, and even

governing authorities outside of the country. Mastercard states: “we may transfer your Personal Information to the United States and other countries which may not have the same data protection laws as the country in which you initially provided the information, but we will protect your Personal Information in accordance with this Global Privacy Notice” (Mastercard Global Privacy Notice, 2018). Although they state that they protect information in accordance with their policy, there is still a possibility that ‘purposes’ in initial collection may not be followed through because third parties may have other purposes that are not be restricted by laws. This also makes it difficult for customers to intercede in the circulation of their data double.

The respective sections of PIPEDA: the obligation for credit card companies to name third parties, the safeguards, accuracy and restrictions placed on the utilization of personal information and the explicit purposes of utilizing personal information, along with the consent of the individual, and prohibition of misleading and deceiving individuals insinuates the attempt to constrain biopolitical practices. Particular the practices of sorting, commodifying and exploiting consumers, yet the potentiality for personal information to be used for ‘other purposes’, as inferred from the credit card terms, illustrates Foucault’s concept of biopolitics in how the assemblage of data doubles could lead to the exploitation of populations (Dillon & Lobo-Guerrero, 2008: 273). Visa and/or Mastercard do not inform customers of new purposes if information has been made available to a different company they are partnered with yet work independently from, “we are not responsible for the content, your use of, nor the privacy practices of those” (Mastercard Global Privacy Notice, 2018). As already noted Mastercard states they “strongly suggest” the customer review the third-party privacy policies (Mastercard

Global Privacy Notice, 2018). Visa also states, "if you are participating in Visa offers or promotions, please also read the privacy notices provided by our partners" (Visa Global Privacy Notice, 2018). The companies mitigate their responsibility over customer personal information and shift the onus onto the consumers to determine that for themselves, yet the utilization of customer information can produce a sense of 'alienation' between the subject and the data generated from the subject (Alterman, 2003: 146). Once personal information is surrendered, and its utilization is consented to, it allows for the potentiality of misuse; granting other parties the use of identifying data for their own objectives (Alterman, 2003: 143; Ruppert, 2011: 227). "Other websites that may be accessible through this website have their own privacy policies and data collection, use and disclosure practices" (Visa Global Privacy Notice, 2018). In other words, the constitution of the consumer's identity, or data double may potentially be jeopardized when the credit card company obtains personal information and makes it available to other parties. Not only does this affect one individual, but also has the potential to affect every consumer who offers their personal information, which implicates the population of consumers. This indicates the biopolitical governance over the population through the construction of these identities; as Van der Ploeg (1999a) states that identifying technologies do not necessarily identify a pre-existing identity, but function as a means of establishing an identity (300). Data can be manipulated, and 'partial' or 'underdetermined' identities constructed, that may be inaccurate, are produced for manufacturing purposes and economic value (Boutin, 2016; Zwick & Knott, 2009: 233). In other words, customer information is not just taken as 'shaped and fixed' but is used to 'produce' identities (Ruppert, 2011: 224). As Foucault (1983) states, "a subject is

not to be subjected (connoting disciplinary power) but to be subjectified" (Rygiel, 2011: 224). Although the terms do not explicitly state customer populations are exploited based on the construction of identities, it can be implied that this could occur. The mention of aggregated consumer reports, other entities having different laws, the notice of third party policies, and the mitigation of responsibility for third party practices and personal information consented to, implies that 'data subjects are produced through other actors that determine their identity and classification' (Ruppert, 2011: 224). Essentially, acting and engaging as a consumer-citizen renders a customer limited in power. Companies acquiring control over the information of populations, and the manufacturing of identities and differentiation as valuable commodities illustrates the workings of biopower; as it is a biopolitical surveillance that manages subpopulations through imperfect representations of identities that creates consequential affects for the individual, and the population (Gates, 2010: 424; Lauer, 2008: 301,320, 321; Lyon, 2003a: 5).

5 Conclusion

This thesis sought to examine the biopolitics of the credit card industry in its governance over the consumer population through consumer-citizenship and the manufacturing of consumers into valuable information commodities. Of particular interest were how biometrics was utilized to securitize identity, and how it enabled the credit industry to obtain and monitor consumer data, and determine risk and value, thereby controlling financial movement and segregating and commodifying the population. The emphasis on neoliberalist principles of self-responsibilization, and entrepreneurship provided a way for the credit card company to minimize threat and maximize economic growth through the production and regulation of the consumer population. Biopolitics, as an umbrella concept, was used for addressing the techniques, inducements, and challenges of governing the consumer-population-body through technology in the name of risk, security and consumerism. This thesis also examined the Visa and Mastercard privacy policies, to examine the articulation of consumer-citizenship and how it enables consumers to securitize identity in response to risk-management and convenient access. As well as how it manufactures consumers into marketing commodities through the collection, use and sharing of data.

The literature revealed that the securitization of identity illustrates biopolitical governance that enables the identification of the consumer-citizen, and division of the consumer population into desirable and undesirable groups, through the collection of data, observation of consumer activity, and regulation and control of financial mobility and consumerism. Biopower constitutes how members of a population are identified through the obtainment of knowledge and continuous examination and calculation of the

behaviour, activities, and contingencies of individuals. It determines the differences in measures of value and risk amongst populations, which are dependent upon the exercise of self-responsibilization. The credit card industry positions the securitization of identity as an act of consumer-citizenship, with emphasis on neoliberal values of self-governance, self-management, self-autonomy, choice and freedom. This process is rendered as an obligatory and peformative act of consumer-citizenship that manages risks i.e. identity fraud, and permits access to entitlements. Biopower, as both constraining and productive, can only act through the exercise of freedom of the citizen. Although several modes of behaviour equate with a neoliberalist exercise of consumer-citizenship, biometric technology in particular is implemented as a biopolitical security apparatus. This technology guards the consumer-citizen's identity from risks, but also functions as a technology of self and freedom that facilitates the optimization of a quality of life, and constitutes a subject as a member of a desirable population. The biopolitical relationship between biometrics and the consumer-citizen enables a calibration of the individual body to the species body by calculating consumer life. It renders the population amendable and productive for the function of the economic condition of the credit card industry.

The development of biometric technology along with the collection and automization of data for the purposes of calculating the economic value and risk of consumer subpopulations illustrates a statistical expertise, a technique of biopower that responds to elements of life through regularization. The financial identity of the consumer is determined through behaviour and probabilities that reveal the competency to engage in circuits of consumption, and culpability of risk. Risk classes, and varying standards of inclusion and exclusion are depicted through statistical credit scoring.

Subjects are rendered as knowable and calculable in relation to the population through a continuous modulation to minimize financial loss and maximize financial gain.
The relationship between biometrics and the data double facilitates the credit card industry's commodification of consumers. These surveillance practices not only function to authenticate identity, but the information extracted through codes is processed and constructed into a particular identity, and thereby a group formed for specific objectives. These technologies enable a 'social sorting' through 'digital discrimination' that reduce identities into subpopulations of risk and value, inclusion and exclusion for particular markets that affect life chances, by limiting or expanding access. They represent an exercise of biopower that renders the consumer population manageable through targeted control practices of commodification and regulation that maximize benefits for financial industries.

The analysis on PIPEDA provides the legal framework for which these credit card companies can act, which revealed that Visa and Mastercard adhere to the federal privacy law. However, the analysis on applicable sections of PIPEDA in accordance with the credit card privacy terms illustrates that generally the sections act to constrain the biopolitical sorting, commodification and potential exploitation of consumer populations. Ensuring customer consent to legitimate purposes on the collection and use of personal information, protection and accuracy of information, guidelines that limit the companies' use and sharing of personal information with third parties represent the recognition of protecting the identity of customers, and the prevention of credit card companies inappropriately manufacturing customers as valuable commodities. The legislation seeks to constrain the neoliberal governance 'at a distance' by limiting self-responsibilization,

self-governance, and self-entrepreneurship of the consumer-citizen and makes companies ultimately responsible over customer personal information. Although it could also be interpreted that by mandating the rights of individuals, for example, ensuring customers can access their own personal information attained by the credit card company and choose to have it amended, enables self-governance over their data double; as responsibilization is placed on the customer to rectify personal information. Furthermore, legislating the opting out of consumerism activities, or on the utilization of personal information ensures the legal right to non-adherence of consumer-citizenship principles of self-entrepreneuship. Yet, the exercise and choice of those labeled irresponsible enables the segregation of the undesirable, facilitating categories of exclusion, which encourages the biopolitical aggregation and sorting of populations. Although there are some variations in how biopolitics can be constrained and also enabled through PIPEDA legislation, the credit card policies are clearly able to biopolitical govern the customer population and mobilize consumer-citizenship through its terms.

This analysis of Visa and Mastercard privacy policies reveals through its terms the emphasis on subjects to securitize their identity for risk management, and access to consumerism. Specifically, there is a prominence on citizenship claims to access and entitlement that mobilizes citizenship practices of providing personal information, engaging in transactions, and opting in for consumerist goods i.e. marketing, products and services; reflecting the principles of self-entrepreneurship and responsibilization. Opting-out of the collection, use and sharing of data is provided, however providing this option operates to exclude and segregate undesirable populations. From the terms, there perceives to be two levels of exclusion. The one is a customer subpopulation that is still

incorporated through a 'principle of activity', meaning they securitize identity by providing personal information, and engaging in transactions, yet opt out of certain circuits of consumption i.e. marketing, services, targeting. The other consists of 'anti-citizens', which do not securitize their identity; they reflect the irresponsible choice and action of consumer-citizenship, thus they forfeit citizenship claims to access and benefits. They are depicted as non-productive to the industry; thereby they reap the 'consequences' of refusing to authenticate their identity. The emphasis on securitizing identity represents the biopolitical process that 'calibrates the individual body to the species body', and the management of the population that identifies and constructs the desirable from the undesirable.

The terms articulate biopolitical governance that mobilizes the customer to exercise citizenship principles of autonomy and freedom. Securitizing identity, consenting to the use and sharing of personal information for the assurance of security, and protection, i.e. identity fraud, authenticating payments and transactions etc., illustrates the responsibilization of risk that lies on the customer. The securitization process also enables the biopolitical management over the population that controls and regulates access through the monitoring of customer behaviour and activities. The credit card industry is able to 'govern at a distance' through the freedom and choice of customers, facilitating a biopolitical apparatus that has a regulatory function to cancel the negative i.e. fraud, and promotes the positive i.e. economic growth. The responsibilization of risk also contains a 'shifting of risk', in which the onus of responsibility over the utilization of personal information is mitigated from the credit card company and transferred onto the customer; illustrating the neoliberal rationale of

risk – prudentialism, in which risk is shared, yet acted upon individually. Consenting to the collection, use and sharing of personal information is an individual responsibility of risk, and ensures blame on the customer. This keeps the customer in a state of subjectification. In other words, by shifting risk onto the customer, they are less able to challenge the procedures and practices of the company. The citizenship claims of freedom that mobilize customers to securitize identity and assume risk endorse apparatuses of control, and governance over the population.

By securitizing identity, customers' enable credit card companies to categorize and commodify their identities, the provisions state that Visa and Mastercard collect and use personal data and share it with third parties. The citizenship activities of customers allows for the construction of identities for particular objectives, like marketing, as listed in the terms. For example, the aggregation of personal information, i.e. shopping behaviour, family status and transactional information coincides with the function of biopolitics that makes populations knowable and visible. An extraction of the 'vital signs' of life that proceeds to sort and manage populations based on value and risk that has effects on their life chances. Although, there is a general awareness that information may be used for security, and targeted marketing purposes, it is unclear if customers are made aware of the credit card company's explicit purposes on the utilization of data, the data that is collected and shared at the time, and the purposes of third party entities. Individuals are not made aware of the potential risks, or effects associated with consenting to the use and sharing of their personal information, nor are they explicitly informed on the lists of third parties their information is shared with, but are instead obligated to determine the risks for themselves. However, it can be implied through the

terms that the construction of partial identities, misuse of data, and exploitation of the customer population is possible. While customers have the opportunity to correct, and prevent the utilization of their data double, it remains difficult for customers to maintain control over it once they have consented to the rules of citizenship, i.e. engaging in transactions, authenticating identity. It is biopower that is exercised when companies acquire control over the information of populations; the manufacturing of identities and differentiation as valuable commodities is enabled and mobilized through consumer-citizenship – which renders the population limited in power. As the promise of freedom coincides with, and manifests control, since power can only be exerted on those that are free.

Analyzing the credit card policy provisions in accordance with the literature provides consumers with the necessary knowledge on how the credit card industry operates within Canada. It addresses how the securitization of identity is applied within the terms, and how consumers are manufactured as information commodities through consumer citizenship. Particularly, it brings awareness and knowledge to consumers to better understand the effects of consenting, and how to prevent the utilization of their personal information. There was an expectation to see biometric information reflected in the policies, although there was no explicit/expressed mention of the use of biometrics. The only implication of it was in the Visa Global Privacy Notice, 2018 section where it states personal information may be collected from third party digital wallets and online merchants when making online purchases. Digital wallets like Apple Pay allow the option to use biometrics when engaging in transactions; this implies that Visa would also receive biometric data. The policies not addressing this specifically could mean that they

simply were not specific enough, or they avoid mentioning the word biometrics as this invokes a grey area. Further, the use of biometrics has not been explicitly addressed within PIPEDA. An unclear understanding or ambiguous knowledge on the collection/use of biometric data hinders the ability of a customer to make an informed consent. For future research, a search of other credit card company policies indicating the use of biometrics would be suggested, along with an analysis on other entities policies regarding the use of personal information, i.e. data brokers, marketing companies, and social media entities. This would provide more detailed data for a more thorough analysis in how populations are categorized, commodified, and discriminated, and the effects of it on life chances.

References

Aas, K.F. (2006). The body does not lie: Identity, risk and trust in technoculture. *Crime Media Culture*, 2 (2), 148-153. DOI: 10.1177/1741659006065401

Agamben, G. (2004). Bodies without words: Against the biopolitical tatoo. *German Law Journal,* 5(2), 168–9. Retrieved from https://static1.squarespace.com/static/56330ad3e4b0733dcc0c8495/t/56b91bd54d088e167441b396/1454971861774/GLJ_Vol_05_No_02_Agamben.pdf

Agar, J. (2001). Modern horrors: British identity and identity cards. In Caplan, J. and Torpey, J. (Eds.), *Documenting individual identity.* New Jersey: Princeton University Press

Ajana, B. (2013). *Governing through biometrics: The biopolitics of identity*. UK: Palgrave Macmillan

Alterman, A. (2003). A piece of yourself: Ethical issues in biometric identification. *Ethics and Information Technology*, 5 (3), 139-150. DOI: 10.1023/B:ETIN.0000006918.22060.1f

American Civil Liberties Union (ACLU). (2004). The surveillance-industrial complex: How the American government is conscripting businesses and individuals in the

construction of a surveillance society. Written by Jay Stanley for ACLU, August. New York: ACLU. Retrieved from https://www.aclu.org/files/FilesPDFs/surveillance_report.pdf

Amoore, L. (2006). Biometric borders: Governing mobilities in the war on terror. *Political Geography,* 25(3), 336-351. DOI: 10.1016/j.polgeo.2006.02.001

Aradau, C and van Munster, R. (2007). Governing terrorism through risk: Taking precautions, un(k)nowing the future. *European Journal of International Relations*, 13 (1): 89-115. https://doi.org/10.1177/1354066107074290

Atkinson, P.A., & Coffey, A. (1997). Analysing documentary realities. In Silverman, D. (Ed.), *Qualitative Research: Theory, method and practice* (45-62). London: Sage.

Balibar, E. (2002). *Politics and the other scene*. London: Verso.

Balibar, E. (2004). *We, the people of Europe? Reflections on transnational citizenship*. Oxford: Princeton University Press.

Beer, D. (2014). The biopolitics of biometrics: An interview with Btihaj Ajana. *Theory, Culture & Society*, 31(7/8), 329–336. Retrieved from https://www.theoryculture society.org/the-biopolitics-of-biometrics-an-interview-with-btihaj-ajana/

Bhandar, D. (2004). Renormalizing citizenship and life in fortress North America. *Citizenship studies*, 8(3), 261-268. DOI: 10.1080/1362102042000256998

Bogard, M. (2006). Surveillance assemblages and lines of flight. In Lyon, D. (Ed.), *Theorising surveillance: The panopticon and beyond.* Devon: Willan Publishing.

Bogard,W. (2007). The coils of a serpent: Haptic space and control societies. *CTheory.* Retrieved from http://www.ctheory.net/articles.aspx?id=581

Boutin, P. (2016, May 30). The secretive world of selling data about you. *Newsweek*. Retrieved from http://www.newsweek.com/secretive-world-selling-data-about-you-464789

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, 9(2), 27-40. DIO:10.3316/QRJ0902027

Boyatzis, R. (1998). *Transforming qualitative information: Thematic analysis and code development.* Thousand Oaks, CA: Sage

Burt, C. (2017, December 6). Visa launches biometrics-focused security roadmap. *Biometric Update.com*. Retrieved from http://www.biometricupdate.com/201712/visa-launches-biometrics-focused-security-roadmap

Butler, J. (2005). *Giving an account of oneself.* New York: Fordham University Press.

Byrne, L. (2007, June 19). *Securing our identity: A 21st century public good*. Retrieved from http://press.homeoffice.gov.uk/Speeches/sc-identity-21st-century

Caplan, J., & Torpey, J. (2001). *Documenting individual identity.* New Jersey: Princeton University Press.

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A.J. (2014). The use of triangulation in qualitative research. *Oncology Nursing Forum,* 41(5), 545-547. DOI: http://dx.doi.org.proxy.lib.uwaterloo.ca/10.1188/14.ONF.545-547

Cavoukian, A. (1999). Consumer biometric application: A discussion paper. *Information and Privacy Commisioner Ontario*. Retrieved from http://www.ontla.on.ca/library/repository/mon/10000/211727.pdf

Cheney-Lippold, J. (2011). A new algorithmic identity: Soft biopolitics and the modulation of control. *Theory, Culture and Society*, 28(6), 164-181. DOI: 10.1177/0263276411424420

CIFAS. (2007). *Identity Fraud.* Retrieved from http://www.cifas.org.uk/default.asp?edit_id=566-56

Coll, S. (2013). Consumption as biopower: Governing bodies with loyalty cards. *Journal of Consumer Culture*, 13(3), 201–220. DOI: 10.1177/1469540513480159

Consumers ready to switch from passwords to biometrics, study shows. (2018). *Visa.* Retrieved from https://www.visa.ca/en_CA/visa-everywhere/security/how-fingerprint-authentication-works.html

Crabtree, B., Miller, W. (1999). A template approach to text analysis: Developing and using codebooks. In Crabtree, B., Miller, W. (Eds.), *Doing qualitative research* (pp. 163–177.) Newbury Park, CA: Sage

Credit card companies plan to sell your purchase data to advertisers. (2011, October). *Out-Law.* Retrieved from https://www.theregister.co.uk/2011/10/27/credit_card_companies_may_sell_your_payment_data_to_advertisers/

Curry, M.R. (2004). The profiler's question and the treacherous traveler: Narratives of belonging in commercial aviation. *Surveillance and Society*, 1(4), 475-99. Retrieved from http://resolver.scholarsportal.info.proxy.lib.uwaterloo.ca/resolve/14777487/v01i0004/102_tpqattnobica.xml

Cybernetics. (n.d.). Dictionary.com Online. Retrieved from http://www.dictionary.com/browse/cybernetics

Daly, J., Kellehear, A., & Gliksman, M. (1997). *The public health researcher: A methodological approach*. Melbourne, Australia: Oxford University Press.

Data triangulation: How the triangulation of data strengthens your research. (2018). *write.com*. Retrieved from http://www.write.com/writing-guides/research-writing/research-process/data-triangulation-how-the-triangulation-of-data-strengthens-your-research/

Deleuze, G. (1992). *Postscript on the societies of control.* Retrieved from http://links.jstor.org/sici?sici=0162-2870%28199224%2959%3C3%3APOTSOC%3E2.0.CO%3B2-T

Dillon, M., & Lobo-Guerrero, L. (2008). Biopolitics of security in the 21st century: An introduction. *Review of International Studies*, 34 (2), 265-292. DOI: 10.1017/S0260210508008024

Dillon, M., & Reid, J. (2001). Global liberal governance: Biopolitics, security and war. *Journal of International Studies*, 30(1), 41-66. DOI: 10.1177/03058298010300010501

Dilts, A. (2011). From 'entrepreneuer of the self' to 'care of the self': Neo- liberal governmentality and Foucault's ethics. *Foucault Studies*, 12, 130-146. DOI: http://dx.doi.org/10.22439/fs.v0i12.3338

Dodge, M., & Kitchin, R. (2005). Codes of life: Identification codes and the machine-readable world. *Environment and Planning D,* 23(6), 851–81. DOI:10.1068/d378t

Dureval, H. (2017, January 23). Growing demand for biometric security in banking. *Mapa.* Retrieved from http://www.maparesearch.com/growing-demand-for-biometric-security-in-banking/

Edelberg, W. (2003). Risk-based pricing of interest rates in household loan markets. Finance and Economics Discussion Series: *Staff Working Papers, United States Federal Reserve Board.* Retrieved from https://www.federalreserve.gov/pubs/feds/2003/200362/200362pap.pdf

Efficient client onboarding: The key to empowering banks. (2013, February) *Cognizant 20-20 Insights.* Retrieved from http://www.cognizant.com/InsightsWhitepapers/Efficient Client-Onboarding-The-Key-to-Empowering-Banks.pdf

Eisner, E. W. (1991). *The enlightened eye: Qualitative inquiry and the enhancement of educational practice.* New York, NY: Macmillan Publishing Company.

Elmer, G. (2004). *Profiling machines: Mapping the personal information economy.* Cambridge, MA: MIT Press.

Epstein, C. (2007). Guilty bodies, productive bodies, destructive bodies: Crossing the biometric borders. *International Political Sociology*, 1(2), 149-64. https://doi-org.proxy.lib.uwaterloo.ca/10.1111/j.1749-5687.2007.00010.x

Ericson, R., Barry, D. & Doyle, A. (2000). The moral hazards of neo-liberalism: lessons from the private insurance industry. *Economy and Society,* 29(4), 532-558. DOI: 10.1080/03085140050174778

Esposito, R. (2008) *Bíos: Biopolitics and philosophy.* (T. Campbell, Trans.). Minneapolis: The University of Minnesota Press.

European Commision. (2005). Biometrics at the frontiers: Assessing the impact on society. *Technical Report Series*. Retrieved from http://www.statewatch.org/news/2005/mar/Report-IPTS-Biometrics-for-LIBE.pdf

Ewald, F. (1991). Insurance and risk. In Burchell, G., Gordon, C. and Miller, P. (Eds.), *The Foucault effect: studies in governmentality*. London: Harvester Wheatsheaf.

Feeley, M., & Simon, J. (1992). The new penology: Notes on the emerging strategy of correction and its implications. *Criminology,* 30 (4), 449-474. DOI: 10.1111/j.1745-9125.1992.tb01112.x

Fereday, J., & Muir-Cochrane, E. (2006). Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International Journal of Qualitative Methods*, 5(1), 80-92. https://doi-org.proxy.lib.uwaterloo.ca/10.1177/160940690600500107

Foucault, M. (1978). The history of sexuality. Vol. 1: An introduction. (R. Hurley, Trans.). New york: Random House. (Originally published La volonté de savoir [Histoire de la sexualité I] in 1976)

Foucault, M. (1980). Two lectures. In Gordon, C. (Ed.), *Power/Knowledge: Selected interviews and other writings 1972-1977* (78-108). New York: Pantheon

Foucault, M. (1982). The subject and power. *Critical Inquiry*, 8 (4), 777-795. https://doi.org/10.1086/448181

Foucault, M. (1983). The subject and power. In: Dreyfus, H.L., & Rabinow, P. (Eds.), *Michel Foucault: Beyond structuralism and hermeneutics.* Chicago: University of Chicago Press.

Foucault, M. (1988). *Technologies of the self.* Martin, L.H., Gutman, H., and Hutson, P.H. (Eds.). Amherst: University of Massachusetts Press.

Foucault, M. (1993). About the beginning of the hermeneutics of the self: Two lectures at Dartmouth. *Political Theory,* 21(2), 203. Retrieved from http://links.jstor.org/sici?sic i=0090-5917%28199305%2921%3A2%3C198%3AATB OTH%3E2.0.CO%3B2-R

Foucault, M. (1994). *The essential Foucault: Selections from essential works of Foucault, 1954-1984*. Rabinow, P., and Rose, N. (Eds.). New York and London: The New Press.

Foucault, M. (1995). *Discipline and punish: The birth of the prison.* (A. Sheridan, Trans.). New York: Random House. (Originally published Surveiller et punir: Naissance de la prison in 1975)

Foucault, M. (1997): The ethic of care for the self as a practice of freedom. In P. Rabinow (Ed.), *Ethics: Essential works of Foucault 1954-1984.* (R. Hurley and others, Trans.). New York: The New York Press. (Originally work published 1987)

Foucault, M. (2000). The political technology of individuals. In J.D Faubion (Ed.), *Power: Essential works of Foucault 1954-1984*. New York: The New Press. (Original work published 1988)

Foucault, M. (2003). *Society must be defended: Lectures at the collège de France, 1975-76*. (D. Macey, Trans.). A. I. Davidson (Ed.). New York: Picador. (Originally published Il faut défendre la société in 1997)

Foucault, M. (2007). *Security, territory, population: Lectures at the collège de France 1977-1978.* (G. Burchell, Trans.). New York: Palgrave Macmillan. (Originally published Securité, territoire, population in 2004)

Foucault, M. (2008). *The birth of biopolitics: Lectures at the college de France 1978-1979.* (G. Burchell, Trans.). M. Senellart (Ed.). New York: Palgrave Macmillan. (Originally published Naissance de la biopolitique in 2004)

Fujitsu (2012). Fujitsu builds Japan's first palm vein authentication system for ATMs" Retrieved from http://www.fujitsu.com/global/news/pr/archives/month/2012 /20120926- 01.html

Gates, K. (2010). The securitization of financial identity and the expansion of the consumer credit industry. *Journal of Communication Inquiry*, 34(4) 417-431. DOI: 10.1177/0196859910377500

Geodemographics. (n.d). Mbaskool.com. Retrieved from https://www.mbaskool.com/business-concepts/marketing-and-strategy-terms/7264-geodemographics.html

Hacking, I. (1990). *The taming of chance*. Cambridge: Cambridge University Press.

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of Sociology*, 51(4), 605-622. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.392.9622&rep=rep1&type=pdf

Hardt, M., & Negri, A. (2004). *Multitude: War and democracy in the age of empire*. New York: The Penguin Press.

Harrer, A. (2016, March 23). Bank of Montreal, Mastercard launch biometric corporate cards in Canada and U.S. *Financial Post.* Retrieved from http://business.financialpost.com/news/fp-street/bank-of-montreal-mastercard-launch-biometric-corporate-cards-in-canada-and-u-s

Hoepfl, M. (1994). *Closure of technology teacher education programs: factors influencing discontinuance decisions.* Morgantown, WV: Unpublished doctoral dissertation.

Hoepfl, M.C. (1997). Choosing qualitative research: A primer for technology education researchers. *Journal of Technology Education*, 9(1), 47-63. https://doi.org/10.21061/jte.v9i1.a.4

Hunt, K., & Rygiel, K. (2006). Introduction: (En)gendering the war on terror. In Hunt, K., & Rygiel, K. (Eds.), *War stories and camouflage politics* (1-24). Burlington, VT: Ashgate

Huysmans, J. (2006). *The politics of insecurity: Fear, migration and asylum in the EU*. London: Routledge

Isin, E. (2004). The neurotic citizen. *Citizenship Studies,* 8(3), 217-235. DOI: 10.1080/1362102042000256970

Isin, E., & Nielsen, G.M. (2008). *Acts of citizenship*. New York: Palgrave Macmillan

Johnson, R. W. (1992). Legal, social and economic issues in implementing scoring in the US. In L. C. Thomas, J. B. Crook and D. B. Edelman (Eds.), *Credit scoring and credit control* (19-32). Oxford: Clarendon Press.

Kant, I., Schneewind, J., Baron, M., & Kagan, S. (2002). *Groundwork for the Metaphysics of Morals* (Wood A., Ed.). New Haven, London: Yale University Press.

Kaye, K. (2013, April 16). Mastercard, AmEx quietly feed data to advertisers. Privacy concerns prevent some targeting options. *AdvertisingAge*. Retrieved from http://adage.com/article/dataworks/mastercard-amex-feed-data-marketers/240800/

Kelly, M. (n.d.). Michel Foucault: Political thought. *Internet encyclopedia of philosophy.* Retrieved from http://www.iep.utm.edu/fouc-pol/

Kristensen, K.S. (2013). *Michel Foucault on bio-power and biopolitics* (Masters thesis, University of Helsinki). Retrieved from https://helda.helsinki.fi/bitstream/handle/10138/39514/Kristensen%20Masters%20Thesis.pdf?sequence=3

Labuschagne, A. (2003). Qualitative research: Airy fairy or fundamental? *The Qualitative Report,* 8(1), 100. Retrieved from http://link.galegroup.com/apps/doc/A172525605/AONE?u=uniwater&sid=AONE&xid=acc26560.

Laissez-Faire [Def. 1]. (2017). In Merriam Webster Online. Retrieved from https://www.merriam-webster.com/dictionary/laissez-faire

La Porte, T. R. (2013). Postscript: Reflections on procedures, trial and error and functional forgiveness. In C. Bieder and M Bourrier (Eds.), *Trapping safety into rules: How desirable or avoidable is proceduralization?* (251-271) Farnham: Ashgate.

Lauer, J. (2008). From rumor to written record: Credit reporting and the invention of financial identity in Nineteenth-Century America. *Technology and Culture,* 49(2), 301-324. Retreived from https://www-jstor-org.proxy.lib.uwaterloo.ca/stable/40061517

Lemke, T. (2011). *Biopolitics: An advanced introduction.* (E.F. Trump, Trans.). New York: University Press. (Originally published as Biopolitik zur Einfüfrung in 2007)

Liñares-Zegarra, J., & Wilson, J.O. (2012). *Risk based pricing in the credit card industry: Evidence from US survey data*. University of St Andrews. Retrieved from https://www.st-andrews.ac.uk/business/rbf/workingpapers/RBF12_001.pdf

Lynch, M. (1998). Waste managers? The new penology, crime fighting, and parole agent identity. *Law and Society Review,* 32 (4), 839-870. DOI: 10.2307/827741

Lyon, D. (1993). An electronic panopticon? A sociological critique of surveillance theory. *Sociological Review*, 41(4), 653-78. https://doi.org/10.1111/j.1467-954X.1993.tb00896.x

Lyon, D. (1994). *The electronic eye: The rise of surveillance society*. University of Minnesota Press. Retrieved from http://www.jstor.org/stable/10.5749/j.ctttsqw8

Lyon, D. (2002). Editorial. Surveillance studies: Understanding visibility, mobility and the phenetic fix. Surveillance and Society, 1(1), 1-7. Retrieved from http://resolver.scholarsportal.info.proxy.lib.uwaterloo.ca/resolve/14777487/v01i0001/1_ssuvmatpf.xml

Lyon, D. (2003a). *Surveillance After September 11.* Cambridge: Polity.

Lyon, D. (2003b). *Surveillance as social sorting: Privacy, risk and digital documentation.* London: Routledge

Lowcards.com. (2012, February 21). Credit card companies sell your personal shopping data. *CTWATCHDOG.* Retrieved from http://ctwatchdog.com/misc/credit-card-companies-sell-your-personal-shopping-data

Makuch, W. M. (2001). Scoring applications. In E. Mays (Ed.) *Handbook of Credit Scoring,* Chicago, IL: Glenlake, pp. 3-21.

Marron, D. (2007). Lending by numbers: credit scoring and the constitution of risk within American consumer credit. *Economy and Society,* 36(1), 103-133. DOI: 10.1080/03085140601089846

Marron, D. (2008). Alter reality: Governing the risk of identity theft. *British Journal of Criminology*, 48 (1), 20-38. DOI: 10.1093/bjc/azm041

Mastercard. (2017). Mastercard-global privacy notice. Retrieved from https://www.mastercard.ca/en-ca/about-mastercard/what-we-do/privacy.html

Mastercard. (2018). Mastercard-global privacy notice. Retrieved from https://www.mastercard.ca/en-ca/about-mastercard/what-we-do/privacy.html

Mastercard and BMO make fingerprint and 'selfie' payment technology a reality in North America. (2016, October 24). *Engagement Bureau*. Retrieved from https://newsroom.mastercard.com/press-releases/mastercard-and-bmo-make-fingerprint-and-selfie-payment-technology-a-reality-in-north-america/

McDermott, V., Henne, K., & Hayes, J. (2017): Shifting risk to the frontline: case studies in different contract working environments, *Journal of Risk Research*. DOI: 10.1080/13669877.2017.1313764

Miller, P., & Rose, N. (2008). *Governing the present.* Cambridge, UK: Polity Press

Muller, B. (2004). (Dis)Qualified bodies: Securitization, citizenship and identity management. *Citizenship Studies*, 8 (3), 279-294. DOI: 10.1080/136210204 2000257005

Muniesa, F., Millo, Y., & Callon, M. (2007). An introduction to market devices. *Sociological Review*, 55(2), 1-12. DOI: 10.1111/j.1467-954X.2007.00727.x

Negroponte, N. (1995). *Being Digital.* New York: Knopf.

Nymi, TD and MasterCard announce world's first biometrically authenticated wearable payment using your heartbeat. (2015, August 11) *Marketwired.* Retrieved from

http://www.marketwired.com/press-release/nymi-td-mastercard-announce-worlds-first-biometrically-authenticated-wearable-2046600.htm

Ong, A. (2006). Mutations in citizenship. *Theory, Culture & Society*, 23 (2-3), 499-505. DOI: 10.1177/0263276406064831

Overview of privacy legislation in Canada. (2014). *Office of the privacy commissioner of Canada.* Retrieved from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/

Patton, P. (1994). Metamorphologic: Bodies and powers in a thousand plateaus. *Journal of the British Society for Phenomenology*, 25(2), 157–69. http://dx.doi.org/10.1080/00071773.1994.11007058

Personal Information Protection and Electronic Documents Act, Statutes of Canada (2000, c. 5). Retrieved from http://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-4.html#docCont

Posadzki, A. (2016, July 26). How Canadian banks are turning to biometrics to use your body to fight fraud. *Thestar.com.* Retrieved from https://www.thestar.com/business/2016/07/22/banks-turn-to-biometrics-to-boost-security-convenience.html

Rabinow, P., & Rose, N. (Eds.). (1994). Introduction. In *The essential Foucault:*

Selections from essential works of Foucault, 1954-1984, vii-xxxv. New York: The New Press.

Reisinger, D. (2011, October 25). Visa, MasterCard to use buying history for ad targeting? *CNET*. Retrieved from https://www.cnet.com/news/visa-mastercard-to-use-buying-history-for-ad-targeting/

Reith, G. (2004). Uncertain times: the notion of ‘‘risk’’ and the development of modernity. *Time and Society,* 13(2), 383-402. DOI: 10.1177/0961463X04045672

Rekola, M. (2013). *Biometrics and banks in Finland from a privacy perspective*. University of Oslo. Retrieved from https://www.duo.uio.no/bitstream/handle/10852/38779/Thesis13_Candidate_8014.pdf?sequence=9

Rice, P., Ezzy, D. (1999). *Qualitative research methods: A health focus.* Melbourne: Oxford University Press

Rose, N. (1999). *Powers of freedom: Reframing political thought.* Cambridge, UK: Cambridge University Press.

Rose, N. (2000). Government and control. *British Journal of Criminology,* 40(2), 321-339. Retrieved from http://www.uio.no/studier/emner/jus/ikrs/KRIM4001/h10/undervisningsmateriale/Artikkel_rose.pdf

Rule, J. (1973). *Public lives, private surveillance.* London: Allen Lane.

Ruppert, E. (2011). Population objects: Interpassive subjects. *Sociology,* 45(2), 218–233. DOI: 10.1177/0038038510394027

Ruppert, E., Law, J., & Savage, M. (2013). Reassembling social science methods: The challenge of digital devices. *Theory, Culture & Society,* 30(4), 22–46. DOI: 10.1177/0263276413484941

Rygiel, K. (2010). *Globalizing citizenship.* Vancouver, British Columbia: UBC Press.

Salisbury, B. (2015, November 6). Biometrics aim to make payments more secure. *Credit Cards.com United Kingdom*. Retrieved from http://uk.creditcards.com/credit-card-news/biometric-verification-1359.php

Salter, M. (2008). Imagining numbers: Risk, quantification, and aviation security. *Security Dialogue,* 39 (2-3), 243-66. DOI: 10.1177/0967010608088777

Stalder, F., & Lyon, D. (2003). Electronic identity cards and social classification. In Lyon D. (Ed.), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination.* Oxon: Routledge

Stanley, J., & Steinhardt, B. (2003). *Bigger monster, weaker chains: The growth of an American surveillance society.* New York: American Civil Liberties Union.

To identify and protect: Advanced enterprise behavioral biometrics. (2017). *Identity metrics*. Retrieved from http://identitymetrics.com

Thacker, E. (2005). *The global genome: Biotechnology, politics, and culture.* Cambridge, MA: MIT Press.

The Federal Trade Commission. (2012, December 18). FTC to study data broker industry's collection and use of consumer data. *News release.* Retrieved from https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/db_201409/#fn4

The Federal Trade Commission. (2014). *Data brokers a call for transparency and accountability*. https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

Trigaux, R. (1982). Direct recognition joining the quill, pen; banks looking for new ways to customer ID—perhaps biometric. *The American Banker,* 29. Retrieved from http://www.lexisnexis.com.proxy.lib.uwaterloo.ca/hottopics/lnacademic/

Turow, J. (1997). *Breaking up America: Advertisers and the new media world.* Chicago: University of Chicago Press.

Use Touch ID on iPhone and iPad. (2017, March 27) *Apple Inc.* Retrieved from https://support.apple.com/en-ca/HT201371

van der Ploeg, I. (1999a). The illegal body: Eurodac and the politics of biometric identification. *Ethics and Information Technology,* 1 (4), 295-302. Retrieved from https://journals-scholarsportal-info.proxy.lib.uwaterloo.ca/details/13881957/v01i0004/295_tibatpobi.xml

van der Ploeg, I. (1999b). Written on the body: biometrics and identity. *Computers and Society*, 37 (1), 37-44. Retrieved from https://dl-acm-org.proxy.lib.uwaterloo.ca/citation.cfm?doid=382042.382051

van der Ploeg, I. (2003). Biometrics and the body as information: Normative issues of the socio-technical coding of the body. In Lyon D. (Ed.), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*. Oxon: Routledge.

van Munster, R. (2005). *The EU and the management of immigration risk in the area of freedom, security and justice*. University of Southern Denmark Political Science Publications. Retrieved from http://www.sdu.dk/~/media/files/om_sdu/institutter/statskundskab/skriftserie/05rens12%20pdf.ashx.

Violino, B. (2015, March 3). Biometric security is on the rise. *CSO*. Retrieved from http://www.csoonline.com/article/2891475/identity-access/biometric-security-is-on-the-rise.html

VISA. (2016). *VISA privacy notice*. Retrieved from https://www.visa.ca/en_CA/legal/global-privacy-notice.html

VISA. (2017). *Visa's future of security roadmap: Australia.* Retrieved from https://www.visa.com.au/pay-with-visa/security/future-of-security-roadmap.html

VISA. (2018). Visa checkout terms of service. Retrieved from https://secure.checkout.visa.com/pages/terms?country=CA&locale=en-CA

VISA. (2018). *Visa global privacy notice*. Retrieved from https://www.visa.ca/en_CA/legal/global-privacy-notice.html

Westin, A.F. (1967). *Privacy and freedom*. New york: Atheneum.

White, A. (2004). Risk-based mortgage pricing: Present and future research. *Housing Policy Debate,* 15(3), 503-531. DOI: 10.1080/10511482.2004.9521512

Whitson, J.R., & Haggerty, D.K. (2008). Identity theft and the care of the virtual self. *Economy and Society,* 37(4), 572-594. DOI: 10.1080/03085140802357950

Williams, M. (2003). Words, images, enemies: Securitization and international politics. *International Studies Quarterly*, 47(4), 511-531. DOI: 10.1046/j.0020-8833.2003.00277.x

Will Apple's iPhone 8 have beefed-up biometrics? (2016, Jan 23) *PYMNTS.com.* Retrieved from http://www.pymnts.com/mobile/2017/samsung-finally-shares-what-caused-note-7-fiasco/

Wilson, D. (2006). Biometrics, borders and the ideal suspect. In Pickering, S., & Weber, L (Eds.), *Borders, mobility and technologies of control* (87-109). The Netherlands: Springer.

Woodward, J., Orlans, N. and Higgins, P. (2003) *Biometrics: Identity assurance in the information age.* New York, McGraw–Hill.

Yin, R.K. (1994). *Case study research: Design and methods* (2nd ed.).Thousand Oaks, CA: Sage.

Zimmermann, Z. (2011, August 23). Data monetization defined. *DELLEMC*. Retrieved from https://infocus.emc.com/zimm_zimmermann/data-monetization-defined/

Zwick, D., & Knott, J.D. (2009). Manufacturing customers: The database as new means of production. *Journal of Consumer Culture*, 9(2), 221-247. DOI: 10.1177/1469540509104375