Trust and Surveillance:
Four Themes and Definitions

By

Stephanie Schutte

Department of Sociology

Lakehead University

Thunder Bay

March 2010

Your file Votre référence
ISBN: 978-0-494-71752-3
Our file Notre référence
ISBN: 978-0-494-71752-3

Table of Contents

Abstract

This is a study that examines the impacts surveillance can have on trust levels in society. The main purpose is to attempt to determine whether surveillance negotiates, manipulates, replaces or damages trust in others.

The method of discourse analysis is used to uncover four dominant themes in surveillance literature – the Panopticon, the synopticon, security and resistance. Questions of trust are posed throughout each section and analyzed by using a single definition of trust. The definitions are derived from four different disciplines – business, sociology, social psychology and philosophy – to create a multidisciplinary and multidimesional perspective on trust. This research contributes to the surveillance literature by reinserting the question of trust.

Surveillance was found not to build or support trust. Rather it acted to manipulate or damage it in each of the major themes. Overall, surveillance may have some of the effects described in Orwell's *Nineteen Eighty-Four*, but it has not completely destroyed trust in each other.

Introduction

"There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized." (Orwell 1962: 3)

George Orwell's character Winston Smith lived under a totalitarian regime where telescreens monitored every move that was made and every word that was said. It was a terrifying image of society where one had to be cautious of even facial expressions as nervous tics, looks of anxiety or "anything that carried with it the suggestion of abnormality, of having something to hide" would end in charges of facecrime (Orwell 1962: 66). Others were also on the lookout for Big Brother, with children turned into "eavesdropping little sneak[s]" who would easily denounce their parents to the authorities (Orwell 1962: 28). The book, originally published in 1949, was oriented towards the future of 1984, with Orwell's speculation about how technology would be used. However, the technology that is available today is significantly more advanced than that imagined for 1984. Has the ability of Big Brother leaning over our shoulders in ways far more intrusive than watching and listening affected our society? Must we really watch our facial expressions in public? Are we turning into spies who report strange actions by others to authorities? Is surveillance making us fearful and cautious around others? How has it changed our levels of trust in others?

Trusting relationships are vital to the proper functioning of society. Without them, we would be left in a situation where there is a "complete absence of trust [which] would prevent [one] from even getting up in the morning" (Luhmann 1979: 4). Trusting relations

built through co presence - "being in the same place with someone else" - have fallen to the wayside with modernity because of the influx of strangers (Lyon 2001: 15). The data gathered by surveillance can be used to create forms of identification that become proxies "for the kind of trust that arises from an ongoing relationship of co present persons" (Lyon 2001: 16). Thus, "[t]he focused and purposeful attention to personal details that we think of as surveillance is a major means of holding together disembodied relationships" (Lyon 2001: 16). Yet relationships that are distant are not the only type that exists as we are constantly put in situations where human contact with strangers is necessary. Though surveillance can be used to connect people, it can also cause issues of distrust and feelings of insecurity in countless ways.

If the surveillance that has made its presence in all forms of daily life only works to damage or destroy trust, how would we be able to get up in the morning? The obvious assumption is that trust is still maintained, but the question is whether the technologies of surveillance can change trust relations. The main point of this thesis is to examine surveillance technology to understand the impact it has on relationships, with a specific focus on how it is affecting our levels of trust in society. Does surveillance negotiate, manipulate, replace, build or damage trust in others?

It is understood that the impact of surveillance on trust has received little to no discussion in social theories of surveillance. To examine the effects of surveillance on trust four key themes in the surveillance literature have been reviewed in order to achieve a better understanding of how surveillance works. Questions of trust were posed throughout the review of key themes to open up areas for the analysis. A discipline was then selected

from which a definition of trust was imported into each of the review sections. These definitions were examined and explained in detail. Finally, attempts were made to answer questions about trust using the selected definitions. This process helped to generate an understanding of how surveillance was impacting on trust. It also demonstrated that trust is a multidisciplinary concept.

Examining the effects of surveillance on trust in this way allowed for a multidimensional introduction of trust that contributes to the surveillance literature. Each key surveillance theme was chosen because of its prominence in the literature and its relevance to trust. The disciplines that provided the definitions and understandings of trust were business, sociology, social psychology, and philosophy. These specific disciplines were selected because they all took into account social aspects of why and how trust is given.

Methodological Strategy

The purpose of this study, to incorporate trust into the dominant themes of surveillance, was accomplished through a process of discourse analysis where "a large patterning of thought" was uncovered (Scott and Marshall 2005: 159). In this case the large patterns of thought were the four main themes chosen from the surveillance literature - panopticism, synopticism, security and resistance - which can also be thought of as dominant discourses in the subject area. These were uncovered through a process of literature review. The injection of concepts of trust into these discursive themes benefited and contributed to them (Shaw and Greenhalgh 2008: 2509). Overall, my strategy is to

rethink surveillance in terms of trust.

One potential limitation to this study is that the multidimensional definition of trust does not convey the exact meaning of trust from the discipline which it was borrowed. Not all the nuances of discipline-specific elaborations on trust were imported. However, in using definitions from different disciplines I wanted to enhance the surveillance literature by asking questions of it that were not being posed. What is perhaps lost in each instance of borrowing from a discipline is gained in the intellectual liveliness of how trust is dealt within each theme.

Selecting Social Surveillance Theories and Definitions

Surveillance in this research can be understood as a way to monitor an individual's or group's behaviour and exchanges in both private and public life through the use of technologies that visually monitor, such as video cameras, or the technologies that monitor spaces in which people are not physically present, such as dataveillance that collects, collates and analyzes personal data (Yar 2006: 142). The numerous types and topics of surveillance made choosing theories a difficult task. However, each topic was selected based on the standing it had in social theories of surveillance and the relevance that it could have on negotiating, manipulating, replacing, building or destroying trust in others. Also, since trust is a concept that has been studied in several different disciplines, there were "a large number of potential definitions" (Whitty and Joinson 2009: 97). Each discipline selected to provide the definition of trust had multiple understandings of trust; however, the attributes taken for the definitions included only forms of trust that employed social

understandings. For example, since psychology focuses mainly on individual cognition, social psychology is more useful because it takes social settings into consideration when analyzing how people make trust decisions.

The conceptual design of the four themes and definitions may be represented in this way:

	Surveillance Themes	Trust Definitions
1.	Panopticism: The classic and the electronic Panopticon	Business: Trust is viewed from a rational-calculative perspective where "increases in trust decrease transaction costs and the converse applies" (Wong 2008: 179).
2.	Synopticism: The parallels of watching and being watched; The virtual world and reality	Sociology: Trust is the belief "that the results of somebody's action will be appropriate from our point of view" (Misztal 1996: 24).
3.	Security: Technology and consumerism; the privatization of the security industry	Social Psychology: Trust is a "generalized expectancy held by an individual that the word, promise, oral or written statement of another individual or group can be relied on" (Rotter 1971: 444).
4.	Resistance: Large or small group and Individual level of resistance	Philosophy: Trust "is in essence an attitude of positive expectation about other people, a sense that they are basically well intentioned and unlikely harm us. To trust people is to expect that they will act well, that they will take our interests into account and will not harm us" (Grovier 1998: 6).

1. Panopticism - Business

The first theory selected, the Panopticon, is the most dominant theme in all social surveillance theories. When discussing any type of surveillance, functions of the Panopticon are more than likely to be related as it "must be the most discussed and debated

theoretical concept" (Lyon 2006a: 44). The Panopticon can be basically conceptualized to encompass situations where the few watch the many. It is a form of power that can exercise control to create docile, productive bodies. This theme has been thoroughly reviewed in chapter one, which moves from the classical analysis of Michel Foucault's work into more modern social surveillance theories from David Lyon, Greg Elmer and Oscar Gandy, that each feature technological advances. Writing in this way allows for a historical understanding of the Panopticon as well as the ability to conceive more recent developments of technology in which functions of the Panopticon can be applied. After reviewing the literature I found that panoptic techniques were mostly used by businesses to collect and piece together information from consumers. Thus, the definition that seems to best fit the theories is derived from the business discipline, where the function of trust in transaction costs is viewed as vital to business gains. Works used to understand trust from the perspective of the business discipline were from Loon Wong, Tamar Frankel and Lyn Von Swol.

2. Synopticism - Sociology

Another key theme is synopticism, which is discussed in chapter two. Though not discussed as widely as the Panopticon, the synopticon has been used to explain some of the reasons why the Panopticon is so broadly accepted in modern society. The synopticon, or the 'viewer society', is the Panopticon in reverse as it means the many watching the few. Thomas Mathiesen, who originally conceptualized the idea, understands the synopticon working with the Panopticon to discipline the body and mind. Interestingly, this theory opens up a range of ideas because the public is given the opportunity to monitor and

scrutinize those in power. To describe and discuss the impacts of the synopticon on society, Mathiesen is discussed along with incorporations from works by Elmer, Hal Niedzviecki and Aaron Doyle who discuss the popularity of watching in general. In this theme, the conceptualization of trust is taken from sociology. Sociology mainly understands trust as a function, so the question becomes whether elements of the synopticism, such as divulging personal information online, provide a base for trust to develop and function. Work from Robert Putnam and Charles Tilly were used in an attempt to answer this.

3. Security - Social Psychology

The third theory examined, security, is a common justification for the use of surveillance technology. It has been selected because of its role in potentially creating or destroying trust. Security eliminates risks which can provide potential for trust to build between individuals. However, at the same time it may also produce feelings of distrust because striving for security can be seen as "an ambivalent project which carries in itself a potential for creating its opposite – a heightened sense of insecurity" (Aas, Gundhus and Lomell 2008: 3). In this way, security plays on levels of trust. After September eleventh (9/11), security has gained increasing importance in the surveillance literature. Chapter three uses works from Daniel Neyland, Didier Bigo, Lyon, Mark Andrejevic and Katja Aas, Helene Gunhus and Heidi Lomell. As risk impacts on individuals, I used the definition of trust from social psychology. Social psychology works well in this area because it concentrates on social settings that impact individual experiences and their overall decision of whether to trust others or not. To attain a conceptualization of trust, discussions from Julian Rotter, Russell Hardin, Toshio Yamagishi, Janet Chan, and John

Mirowsky and Catherine Ross are used.

4. Resistance - Philosophy

The fourth and final chapter contains a discussion of resistance. Resistance is a type of oppositional force that is used against power or those who exercise power. Surveillance can be understood as a form of power, and where power is exercised resistance will always be found. Resistance is interesting because it is executed against surveillance on a daily basis and performed by random, ordinary people. It can hold obvious issues of trust as those who resist or rebel may be motivated by the distrust they feel about those using surveillance technology. Also, those who resist may be viewed as untrustworthy, as having something to hide, by companies, the government or society. In discussing this theme, works from Foucault, Lyon, Majid Yar, Gary Marx, Gary Genosko and John Gilliom were used. Trust has been defined using the discipline of philosophy because it takes the context of the situation into consideration. This is important because the context for those who resist differ greatly. Philosophy also looks deeply into reasons for distrust and the effects of techniques that are used to guard against these feelings. Philosophical works from Tom Bailey, Trudy Grovier, and Onora O'Neill are discussed in this section.

Chapter 1

The Panopticon and Trust

In his chapter "Panopticism", Foucault describes how power can be exercised by a disciplinary mechanism in two ways. A disciplinary mechanism is used to fix a mass of people as it "arrests or regulates movements; it clears up confusion; it dissipates compact grouping of individuals wondering about the country in unpredictable ways; [and] it establishes calculated distributions" (Foucault 1977: 219). The first method requires an extraordinary evil, such as the fear and panic caused by the plague, for the disciplinary mechanism to take effect (Foucault 1977: 199). Foucault demonstrates how documented procedures from the seventeenth century demanded the proper functioning of rights and laws during this time of disorder and confusion. These orders held strict divisions during the plague, with each person assigned a 'true' name and 'true' body, and allowed the "penetration of regulation into even the smallest details of everyday life" (Foucault 1977: 198). Individuals were ordered to stay in their houses, locked up by syndics, where "each individual [was to be] fixed in his place. And if he [moved], he [did] so at the risk of his life, contagion or punishment" (Foucault 1977: 198). Power was to be exercised "according to a continuous hierarchical figure, in which each individual is constantly located, examined and distributed among the living beings, the sick and the dead" (Foucault 1977: 197). Ironically, the massive death and destruction caused by the plague were met by an order that held the ideas of a political "utopia of the perfectly governed city" (Foucault 1977: 198). Unfortunately, this model required an exceptional situation to mobilize power (Foucault 1977: 205). It does not allow for a regular functioning (Foucault

1977: 205). However, the second method to exercise power through a disciplinary mechanism only required the right type of architecture. This was in the form of the Panopticon, which can "be understood as a generalizable model of functioning; a way of defining power relations in terms of the everyday life of men" and women (Foucault 1977: 205). This section will explain the classic literature on the Panopticon to describe its features and functions. Following it will be a discussion on the electronic Panopticon and modern interpretations of Foucault's work for an understanding that is relevant to current situations of surveillance. This will make the discussion of trust also relevant to contemporary concerns of surveillance.

Published in 1791, Jeremy Bentham believed his design of the Panopticon prison held the promise of "'the only effective instrument of reformative management'" (Lyon 1994: 63). Foucault argues that this design can achieve prisoner reformation through its ability "to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power" (Foucault 1977: 201). The key to reaching this principle lies in its mechanism of surveillance. The prison is designed so that each prisoner is isolated in a cell that is placed around a central tower (Foucault 1977: 201). The light from the back of the cells ensure each prisoner is visible to the guards who, "through a complicated arrangement of lanterns and apertures, is rendered opaque" (Whitaker 1999: 33). The silhouette of the guards reminds prisoners of a continuous presence that conveys to inmates that they may always be watched; however, because of the darkness, prisoners are uncertain about who is watching or when they are being watched (Whitaker 1999: 33). Thus, the prisoners "are caught up in a power situation of which they are themselves the

bearers" (Foucault 1977: 201). "As the prisoners fear that they may be watched, and fear punishment for transgressions, they internalize the rules" become obedient and self monitor their behaviours (Whitaker 1999: 33). Foucault states that through this "Bentham laid down the principle that power should be visible and unverifiable" (Foucault 1977: 201).

Although this design was not adopted by anyone in Bentham's time, to Foucault it held greater implications than mere prisoner reformation, as he claimed it was "destined to spread throughout the social body; its vocation to become a generalized function" (Foucault 1977: 207). The Panopticon's mechanism of observation gave it efficiency and the ability to penetrate into behaviour, making it a useful tool to train and discipline in institutions other than the prison (Foucault 1977: 204). In fact, Bentham "specified that the principle of the Panopticon could and should be extended to various bounded sites of human activity, from asylums to the eighteenth-century equivalent of welfare institutions, to workplaces, to schools" (Whittaker 1999: 33). Used in the workforce, the Panopticon has the ability to "increase aptitudes, speeds, output and therefore profits" while still maintaining a moral influence over behaviour of the workers (Foucault 1977: 210). In schools, the Panopticon has the ability to fortify students by developing observation skills, writing skills and prompt habits all while preparing the children for the workforce (Foucault 1977: 211). It fits so adequately in other institutions because the Panopticon is not just a piece of architecture, but "the diagram of a mechanism of power reduced to its ideal form [...] it is in fact a figure of political technology" (Foucault 1977: 205).

The diagram is significant because it perfects the exercise of power for several

reasons. First, the Panopticon "can reduce the number of those who exercise it [power], while increasing the number of those upon whom it is exercised" (Foucault 1977: 206). Second, the type of surveillance makes it possible to intervene at any moment because the fear of punishment and scrutiny is a "constant pressure [that] acts even before the offences, mistakes or crimes have been committed" (Foucault 1977: 206). Third, the Panopticon acts directly on the individual giving "'power of mind over mind'" without any need for physical instruments to intervene (Foucault 1977: 206). Fourth, its strength is that "it is exercised spontaneously and without noise" (Foucault 1977: 206). The Panopticon rules out the need for a single power, such as a king, because it is subtle and can be "exercised continuously in the very foundations of society" (Foucault 1977: 208). The role of the inspector can be played by anyone who can observe no "matter what animates him [or her]: the curiosity of the indiscreet, the malice of a child, the thirst for knowledge of a philosopher who wishes to visit [a] museum of human nature, or the perversity of those who take pleasure in spying and punishing" (Foucault 1977: 202). Teachers, for instance, can monitor and scrutinize the behaviours of students. They also have the ability to scrutinize parents as well through student behaviours (Foucault 1977: 211). This power extends to include concerned neighbours who might be questioned or possibly comment on routines implemented by parents (Foucault 1977: 211). Like the inmates in the Panopticon prison, parents may become anxious of who is watching and thus begin to self monitor their actions and internalize the rules to avoid punishment or unwanted scrutiny. All of these features make the Panopticon an easily adaptable, efficient and generalizable model of power.

The Electronic Panopticon

Increasing the reach of the Panopticon are "all systems of visibility that enable a few isolated watchers to scrutinize the behaviour of large groups" (Haggerty and Ericson 2006: 27). Going beyond types of architecture are modern technical advances that permit surveillance Foucault only hinted at and "Bentham could never even have dreamed" (Lyon 2006a: 44). It is argued that new "electronic technologies permit the perfection of [the] Panopticon, but now through software architectures" (Lyon 2001: 114). Surveillance can now come in the form of pen spy cameras and cell phone conversation recorders that can be used at anyplace and anytime. They "complete the panoptic project both by bringing more behaviours to light, and by rendering the surveillance apparatus more opaque" (Lyon 2006a: 44). And with technology's increased use, the mechanism of the Panopticon spread beyond simple bounded spaces "where normalizing hierarchical systems were concentrated" (Haggerty and Ericson 2006: 29). It has enabled a collection of data that is visual, aural and textual which can span across the globe, thus making "discipline no longer limited to single buildings and observation no longer limited to line of sight" (Gandy 1993: 23). Observation actually becomes continuous and extremely subtle because of the development of small surveillance devices. Also, panoptic functions, such as information gathering, are enhanced by new technologies as they can be used to attain personal, decontextualized data that can be used to exercise power. These relations of electronic tools to panopticism are made throughout the surveillance literature because the Panopticon is "capable of interpretation in a number of ways, and of course draws on the

major problematics of modernity" (Lyon 2006b: 4). In the following section, interpretations of the panoptic literature will be examined along with the functions of the Panopticon as described by Foucault. The social theories of surveillance from Elmer and Gandy will provide these interpretations. Questions of trust will then be inserted where applicable to allow for an analysis by the business literature on trust to see if the panoptic technology is replacing, negotiating, manipulating or destroying trust. How does this type of surveillance affect the levels of trust in society between its members, governments and organizations?

Modern Panoptic Theories

In *Profiling Machines*, Elmer discusses how the automation of power in panopticism resembles the illusion of choice on the Internet. He states that a "number of techniques are used to solicit information from users," such as consumers cards that accumulate points through use (Elmer 2004: 38). But he questions whether consumers can be conceived as either "conscious or willing 'participants'" in their own surveillance (Elmer 2004: 38). Upon the addition of rewards and punishments, the automation of power becomes clear. "Shoppers, for example, who decline or merely neglect to sign up for bar-coded discount cards end up paying a significantly higher price for an increasing array of products" (Elmer 2004: 38). In this way, "even if consumers know that information is being collected on them" they must chose participation or face the consequences and pay higher prices (Elmer 2004: 38). Coercion hangs in the background as with the prisoners who chose obedience to avoid punishment in the Panopticon prison. This "incentive to 'opt

in' refers to the 'illusion of voluntariness'" (Elmer 2004: 38). It shows how the technology is automating the collection of data through its 'choice' to divulge personal information, leaving business arguments of enticement "somewhat clouded by a coercive definition of panoptic surveillance" (Elmer 2004: 38).

In addition, Elmer discusses how Internet browser cookies are another way Website owners can automate the collection of a user's personal information. A cookie is a type of surveillance mechanism in which small bits of information are stored on a web browser's memory and on the user's hard drive when a website has been accessed and closed (Elmer 2004: 117). "Cookies essentially provide servers (and their owners) a means of identifying repeat visitors to their Web sites, and in doing so they fundamentally challenge the ability of users to remain anonymous on the Net" (Elmer 2004: 118). Supporters of this tool claim that cookies share only a small amount of information between the user and the Web site owner; however, when it is linked to other types of data, such as personal information divulged by the user, "the relatively small amount of information transmitted by cookies [is] greatly enhanced" (Elmer 2004: 119). When Web browsers began offering options to warn users about sites requesting cookies, users began realizing their limitations (Elmer 2004: 122). Those who preferred not to leave a cookie trail on a Website would be informed of an error on the page (Elmer 2004: 131). "With the help of a default set on 'Accept cookie' preferences and cookie options that significantly limit, disable, or disrupt the convenient flow of relevant online information and services, the release of personal online information has now become either an automatic or forced 'choice' for PC Web users" indicating a type of coercive panoptic technology (Elmer 2004: 131). In the case of

cookies, trust may not be an issue because it is automated; there is no choice. Since the Internet is such a large part of our everyday lives, choosing not to use it because of fear of the collection of data may make life very inconvenient. Trust is an issue after being coerced into opting in. Certainly it is more beneficial to opt in for discount cards, but the relationships between those organizations and consumers must be lasting in order for consumers to keep purchasing and providing information. Thus a question of trust can be raised about whether online businesses need to maintain trust within this illusion. How can they foster trust while their main goal seems to be collecting information?

Besides automating behaviours, another function of the panopticon is its ability to do the work of a naturalist where "the animal is replaced by man" (Foucault 1977: 203). This is because observation makes possible classification, characterization and differentiation, as well as being able to identify, sort and label individuals (Foucault 1977: 203). Gandy examines a technique called data mining that reflects these functions. "Data mining is the process that has as its goal the transformation of raw data into information that can be utilized as strategic intelligence within the context of an organization's identifiable goals" (Gandy 2005: 364). With its primary concern being prediction, "data-mining efforts are directed towards the identification of behaviour and status markers that serve as reliable indicators of a probable future" (Gandy 2006: 364). Once gathered together, the information is sorted into patterns by practices of sorting, classifying and differentiating, then it is used to see relationships and trends (Gandy 2006: 368). "These patterns may allow distinctions to be made between persons, behaviour and outcomes on the basis of relations between the attributes of each" (Gandy 2006: 368).

Therefore, consumer profiles are built based on behaviour online and offline to be able to better predict the individual consumer's tastes, needs and purchasing habits (Gandy 2006: 366). Decisions can be quickly made about which advertisements should be directed to consumers through categorization methods used to determine possible interests in products (Gandy 2006: 366). These efforts at collecting and sorting data have been confirmed successful as "users of customer-profiling systems report dramatic improvements in the productivity of their websites" (Gandy 2006: 366).

Though data mining is closely related to the functions of the Panopticon in its abilities to sort, label and classify, its success reflects another function that can cause damage to the life chances of targeted individuals. One of Gandy's primary concerns with data mining is the way "in which discrimination in information markets reinforces disparities in the level and impact of participation in the public sphere" (Gandy 2006: 377). Since there are "no guarantees that the information acquired from database vendors or consolidators will be accurate" errors in classification or sorting may cause frustration or even substantial problems to specific consumers (Gandy 2006: 377). The ability to alter life chances through denial of access based on 'objective' observations draws on features of the Panopticon. They resemble the use of the Panopticon "to alter behaviour, to train or correct individuals"; its potential to be a laboratory of power (Foucault 1977: 203). "The traditional challenge for data miners is to determine which customers are more valuable, and therefore worth keeping" (Gandy 2006: 364). Companies can alter consumer behaviour as they can deny access to consumers who display risky or unruly behaviour. For example, to prevent business losses, companies will watch for missed payments or other

signs of 'bad behaviour' and begin to deny some customers the ability to sign up or purchase an item (Gandy 2006: 364). Furthermore, even though problems with databases and interpretations of data exist, many corporations have also voluntarily provided "government agencies with access to information out of some heightened sense of patriotism" (Gandy 2006: 375). Combined with the power of security agencies to control access to freedoms and rights, errors could certainly cause frustration and detrimental damage to people viewed as risky based on their consumer profile. Gathering abstracted data and labeling it in technical ways exacerbates these problems as "discriminatory acts that would be declared illegal if they relied solely or primarily on the use of 'suspect categories' like race gender or national origin" may increase because these "meaningful categories have been replaced by coefficients assigned to variables or explanatory factors" (Gandy 2006: 378). These new factors are "less likely to attract the heightened scrutiny of the courts" (Gandy 2006: 378). Not only does this mean that behaviours can be categorized and sorted, but also that they are abstracted from context and thus lose important understandings. It enhances control opportunities over certain groups who would otherwise be protected.

Helping the functions of the Panopticon, Foucault spoke of disciplines as a type of specialized power that could help the movement from "the enclosed disciplines; a sort of social 'quarantine' to an indefinitely generalizable mechanism of 'panopticism'" (Foucault 1977: 216). Disciplines, such as psychology and sociology, can accumulate knowledge that when linked together and extended make "it possible to bring the effects of power to the most minute and distant elements. It assures an infinitesimal distribution of power

relations" (Foucault 1977: 216). Observation and investigation through different techniques help disciplines accumulate knowledge in both the areas of natural and human science that, in turn, generates power (Foucault 1977: 226). Foucault explains the danger of the intermingling of the disciplines: "These techniques merely refer individuals from one disciplinary authority to another, and they reproduce, in a concentrated or formalized form, the schema of power-knowledge proper to each discipline" (1977: 226-227). The disciplines allow "investigation[s] that [are] without limit to a meticulous and ever more analytical observation" (Foucault 1977: 227).

Technology aids in the distribution of information, making it accessible to both experts and amateurs. This strengthens not only the power of the disciplines, but the overall power and control of people outside of those disciplines as well. Gandy explains that data mining "is a small but rapidly expanding specialty within the field of applied mathematics that seeks to derive meaningful intelligence from the analysis of patterns within the sets of data" (2006: 367). Certain sets of skills in descriptive and multivariate levels of statistics are required to be able to use the data in various ways (Gandy 2006: 367). However, new technologies offer online analytical processing tools to "make it easier for subject area specialists who are not familiar with advanced statistical techniques" to use and understand the complex data analysis programs (Gandy 2006: 368). Also, the "diffusion of analytical capacity has been enabled in part by increases in the diffusion of relatively inexpensive computing power to desktop and even to laptop computers" (Gandy 2006: 368). Thus, not only has the information become available for other experts in different areas, but it also has become easier to access from virtually any location. Furthering the expansion of this

information are new systems "that enable the capture, storage and retrieval of information that have become more efficient, less expensive and less demanding of specialized training" (Gandy 2006: 371). This means that people in different disciplines and even people with no training at all can retrieve this information and use it to their benefit as well.

The Panopticon and Trust

There are only small gaps where trust can be placed in the theory of the Panopticon as information seems to be automatically collected, without choice. The abstraction of data allows categorization processes to take over that also do not require trust. Thus, trust-based relations between the information collectors and the watched are limited. However, there may be room for trust in the ability to collect personal information by businesses through the "illusion of voluntariness", as Elmer has suggested. This is because in order for businesses to routinely collect patterns of behaviours consumers must be continually active in their purchasing habits after the initial information has been gathered. Businesses would need to maintain good relations with customers so that information can be continually collected and processed. In building these kinds of relations customer trust is gained. How do online businesses build relations that foster trust? Do they make any attempt to foster trust at all? Online businesses have been chosen as a focus because most of the data collection processes discussed above refer to electronic processes. Also, online businesses have grown exponentially, making the analysis relevant to everyday life.

Trust in the Business Discipline

Trust in the business discipline is "often viewed from a rational-calculative" perspective (Wong 2008: 179). This means that trust is measured to determine the range of benefits, where "increases in trust decrease transaction costs and the converse applies" and, as such, trust is able to "mediate and manage risks" (Wong 2008: 179). In most cases, trusting seems to bring about the best benefits both to companies and consumers. In trusting, it has been found that " when each of us can relax her guard a little, what economists term 'transaction costs' - the costs of the everyday business of life, as well as the costs of commercial transactions - are reduced" (Putnam 2001: 135). Online, where businesses often believe that they are involved in an interaction that is "one of collecting online data first and selling goods, second", trust allows returning customers, lengthened stays on Websites and a more attractive reputation to form trust among other potential clients (Wong 2008: 181). It can also be beneficial to businesses as a source of social capital which consists of "networks of cooperation and mutual trust" that taken together can reap tangible economic gains and returns (Putnam 2001: 324).

Facing decreases to trust, or "when we can't trust our employees or other market players, we end up squandering our wealth on surveillance equipment, compliance structures, insurance legal services, and enforcement of government regulations" (Putnam 2001: 325). Businesses that decide it is more beneficial to abuse trust may suffer a loss of customers as "the more people have heard or read about the use or potential misuse of computerized information about consumers, the more they are concerned about threats to privacy" and may not put their trust in the business (Gandy 1993: 230). Further, mistakes can cost customers and reputation as well. For instance, when information was lost by a

government institution, people "felt that personal data held by the government was at risk" (Goold 2009: 214). In effect, while unlikely causing generalized distrust, these types of losses "may make it harder for certain institutions to operate", as in the case of the government institution where "fewer and fewer members of the public were willing to disclose sensitive, personal information" (Goold 2009: 214). These reasons may make business owners more interested in maintaining trusting relations and better motivated to find ways to protect that trust. Thus, trust in both an online and offline business is still very important. Gathering information or using panoptic techniques to collect information may not work without trust because consumers may not continue to purchase items or services, provide valuable information or boost reputation that could benefit businesses.

Trust Online: Problems and Issues

There are several problems faced by online businesses in the attempt to gain trust from consumers. One problem is that the online business "industry moves so fast that it is very seductive to start thinking in the compressed perspective of 'Internet time' in which things move faster, change quicker, and become outdated almost immediately or blurred" (Wong 2008: 179). These varying fluctuations may make it difficult to build a relationship with consumers because the "relatively stable aspects of business which would make strategies, decisions and plans firmer" are too easily ignored (Wong 2008: 182). Consumers may not be so willing to divulge a large amount of information to online companies because "companies that profess to be reliable and dependable can appear and disappear in an instant, jeopardizing many of their [consumers'] personal and economic

details" (Wong 2008: 177). This leads to another problem which is that people view the Internet as a distrustful environment to begin with. This may be a major issue for businesses to overcome because "the greater the uncertainty and risk in a relationship, the more important the need to establish trust" (Van Swol 2006: 138). People are aware that the "Internet has created boundless opportunities to deceive [where] fake products can now be sold more easily and better protected from detection" (Frankel 2006: 104). In addition, "media stories about internet fraud fuel people's anxiety" (Van Swol 2006: 139). It is a place where "frauds, on-line scams, hacking and phishing [the act of sending email that claims to be from a legitimate organization to acquire sensitive information] are common occurrences and the everyday consumer is increasingly concerned over breaches of privacy and security" (Wong 2008: 177). Moreover, the gap between online and offline reality acts to inform consumers that "the rules and knowledge that have informed our everyday experiences are not seen to apply and as such it [the Internet] is a place of potentially high risk" (Wong 2008: 177). And because "online communication is more impersonal and has less richness due to lack of non-verbal cues and other reductions in social information" it may be hard to build trust (Van Swol 2006: 136). As Frankel states, it is a place where daily email scams "create for me an environment that teaches suspicion and warns me to be on my guard" (2006: 103). Thus, maintaining relationships, collecting data and building trust online may not be so easily performed because the feelings of risk in consumers may cause them to withhold trust from businesses.

To help build trust online, there are techniques businesses use. Wong suggests five methods that businesses can use to gain forms of online trust. These methods involve the

use of "community, flow, brand identity, personal experience, and the idea of institutions" (Wong 2008: 182). Online Web communities help to develop relationships because they incorporate feelings of belonging and membership that "can enable businesses to grow and develop when properly harnessed" (Wong 2008: 183). Flow is the level of involvement which concerns a "highly enjoyable state of consciousness that occurs when our perceived skills match the perceived challenges we are undertaking [where we can] lose our sense of self and time is distorted" (Wong 2008: 183). This feeling occurs in businesses such as eBay where the "users' involvement with the site increases the amount of time they will spend on it, and makes the likelihood of their returning often" (Wong 2008: 184). Brand identity can also help deal with relations between consumers and businesses because consumers may sometimes "rationally depend on brand names in making their personal decisions" to trust (Wong 2008: 184). It can aid in situations of distrust as well because familiarity or trusted brands of security will "act to minimize the effects of [potential] wrong behavior" and ensure a user that there is less risk in making the online purchase (Wong 2008: 185). Personal experience entails the "growth in tolerance towards the variability of service [where] for example, the occasional mix up in order or slightly delayed delivery" is viewed as acceptable "so long as recompense is made and apology is offered" (Wong 2008: 186). Where trust is low in the beginning stages, it can also develop through services that reduce uncertainty such as "well formulated and displayed return policies" (Wong 2008: 186). However, personal experience forms only "as the trust relationship builds through successive and successful interactions [upon which] more informal transactions can be comfortably entered into" (Wong 2008: 186). Finally, trust

can be built by the idea of institutions, such as law and regulation, where "in the Internet context, beliefs that there are legal and regulatory protections for consumers clearly influence and effect trust to be built and developed" (Wong 2008: 186).

Genuine Trust or Manipulation?

Even when trust is gained between buyers and sellers, it is not known whether the techniques used to generate trust are in the best interests of consumers. And if it is the case that trust is developed for the purposes of self-interested business owners who choose to abuse trust, this illustrates the manipulation of trust. In his chapter "Rising Opportunities and Temptations" Frankel states that self-interested business owners are becoming more common partially because of changes in culture that created "lower and weakened counter pressures to prevent gains by deceit and abuse of trust" (2006: 88). He argues that this, in turn, permitted companies to become more accustomed to "antisocial habits and patterns of behaviour" such as greed and envy (Frankel 2006: 88). Morals and values have been weakened with this change as well, affecting the ability to resist temptations and the abuse of trust. Morality is a barrier to the abuse of trust because it helps to "exercise self-control over behaviours" (Frankel 2006: 105). People who are moral are more likely to be trusted because they can "exercise self-control in the face of temptation" (Frankel 2006: 107). However, morality has weakened because its foundations have weakened as well. There have been decreased feelings of empathy, guilt and shame. Technology and surveillance limits these feelings because of their power to take the context out of situations and transform people into numbers. Converting people into numbers changes perspectives and

makes it difficult "to empathize with each of them [employees, consumers and other shareholders] or even empathize with them as a group [because] generally numbers don't raise feelings of empathy" (Frankel 2006: 111). Also, the growing use of technical terms with surveillance creates labels for systems or people which erase of feelings of shame or guilt. For example, "words like 'downsizing an enterprise' blur the reality of anxious and suffering people who lose their livelihoods" (Frankel 2006: 111). Thus, how surveillance changes language and images in panoptic ways can lower feelings of empathy, guilt or shame "in people who naturally possess it" (Frankel 2006: 111). Overall, Frankel's outlook gives the impression that where techniques of panopticism are used - in the form of data mining which provides different meanings to labels and a perspective of numbers - trust seems to be manipulated to achieve the personal goals of business owners. Consumer interests are seemingly insignificant. However, there are other forms of information online that can help make true business interests transparent, such as the Website for the Better Business Bureau, which "exist[s] so consumers and businesses alike have an unbiased source to guide them on matters of trust" (Better Business Bureau). Transparency can force businesses to behave in trusting ways so as to maintain customer relations, and can be used to demonstrate how surveillance can work to bring forth greater trust.

Transparency and Trust

Since the profiles of users, including their "preferences and interests" in dealing with online businesses "are formed progressively as they use services", trust must be maintained between businesses and consumers (Kumpost and Matyas 2009: 1). The

Internet provides a base of information about businesses which consumers can use to make decisions about whether to trust a company or not. As on eBay, transparency can allow buyers to "establish a calculated form of trust and choose among sellers based on their reputations"; consumers may also choose to find information about businesses to calculate trust and potential risk (Van Swol 2006: 137). Examining the relationships on eBay, which uses individual-to-individual transactions, can provide a good example to see what the differences can mean between trustful and distrustful online business relations.

eBay is an auction Website designed in a way so that ordinary people can buy and sell items at their own discretion. It is a market that lacks strict regulations where "individuals [are able to] experience more risk and certainty" (Van Swol 2006: 139). To help reduce these experiences, eBay set up four controls as a form of security to make trading 'safe' on the site (Robinson 2006: 133). These safety features include the Feedback Forum, free fraud insurance for up to $200 worth of goods, a Safe Harbor staff that protects the site from abuse, and an escrow service that acts as a third party to protect buyers and sellers (Robinson 2006: 133). However, "the most popular and effective of these latter solutions is eBay's Feedback Forum system" which is a "public rating system in which people post back their complaints and compliments for all others to view" (Van Swol 2006: 139, 140). These ratings are left by "the highest bidder and the seller [who have] up to ninety days to leave one another feedback as positive, negative, or neutral and to leave an accompanying message of up to eighty characters" (Van Swol 2006: 140). These feedback forums are available for all interested buyers and sellers to read thus helping "foster trust between buyers and sellers by reducing the uncertainty of interacting with an anonymous

stranger over the internet" (Van Swol 2006: 140). It also helps to "discourage fraud by allowing people to spread the word about fraudulent behaviour" (Van Swol 2006: 140). It is a type of surveillance that "grants members strong power to monitor and sanction one another" by either deterring or leading people to buy or sell items (Van Swol 2006: 141).

Resembling the temptation faced by business owners, there may be temptation to abuse the trust on eBay as anonymity allows a person "not to feel obligated to maintain a relationship or interact with that person [the seller for example]"; however, the transparency of reputation provides a clear sign of dishonest acts (Van Swol 2006: 142). Negative feedback has a "more detrimental [effect] on the price a seller could command for more expensive items than for lower-priced items" (Van Swol 2006: 146). It also hurts selling because the enormous amount of members on eBay makes it "easy to find alternate trading partners if one person proves untrustworthy" (Van Swol 2006: 149). Those who maintain positive reputations can reap tangible benefits as research suggests that a seller's "positive reputation increases the final bid amount" (Van Swol 2006: 142). Also, research has found that sellers with positive reputations had "buyers who were willing to pay more" (Van Swol 2006: 146). This transparency grants members the power to monitor and make decisions to trust based on calculation. What is important in this case is that "establishing trust is a necessary condition for both online individual-to-individual transactions and business-to-consumer transactions" to ensure that people feel safe in continuing to enter into virtual business transactions (Van Swol 2006: 147). Thus, trust is necessary to consistently collect information, and it can be built online via trust techniques, positive experiences and transparency. Whether it is being manipulated or not, trust helps put the

panopticon into action.

The Panopticon, Business and Trust

The illusion of voluntariness as described by Elmer permits the opting in of users by eliminating the choice that consumers feel they have. This allows online businesses to gather information about consumers and apply panoptic techniques, such as using the information to determine which users to keep and which to exclude. However, a company must be able to maintain relations with consumers in order to continue to exercise power and attain flows of valuable information. Trust can be gained by using online trust building techniques that ensure consumers have positive experiences and maintaining a good reputation for consumers to see. The transparency and rewards of having good trust relations with consumers may be a deterrent from the abuse of trust for some business owners. Still, the illusion of voluntariness might also entail an illusion of trustworthy businesses because some business owners are caught up in their own goals and personal interests. In this case trust can be understood as being manipulated through the various techniques, experiences and reputations used to build trust. Most of the business literature seems to suggest this abuse of trust as even Wong states that businesses "invariably [are able to] manage their customers and socialize them into acceptable institutional arrangements" after gaining trust (2008: 188). If this is actually the case then consumers should be wary about how much information they divulge after opting in to any company. It demonstrates how in most circumstances the trust of consumers may be manipulated by online businesses.

Chapter 2

The Synopticon and Trust

When the panoptic prison principles are actually put into play, such as in the development of Kingston Penitentiary, the results have been controversial "both for its treatment of prisoners and for their responses" (Lyon 2006b: 5). What actually occurs is "some seemingly curious reversals of panoptic principles in behaviours" (Lyon 2006b: 5). Prisoner's behaviours go from "self-mutilation - one deliberately and repeatedly hits his hands on a stone wall in an exercise yard, causing laceration and bleeding" to "faeces throwing and smearing" (Lyon 2006b: 5). These are acts of extreme resistance diagnosed as "behaviourally disturbed" (Lyon 2006b: 5). Rather than producing docile bodies, these acts demonstrate the subversion of "not merely the immediate situation, but also, by extension, the basic seeing/being seen dissociation that the panopticon is intended to sustain" (Lyon 2006b: 6). Lyon explains that this phenomenon represents "the sharp end of the panoptical spectrum"; what he views as the softer version of the Panopticon can be seen through areas of consumption and entertainment where "[t]he apparently least-panoptic forms of surveillance are ones in which a paradoxical docility is achieved in the name of freely chosen self-expression" (Lyon 2006b: 6). Here, Lyon is making reference to a change of attitudes in being watched at which point "[t]here is a reward for displaying your body and its activities" (2006b: 7) This typically entails the use of the mass media, a source of entertainment which demonstrates that "it is gratifying to be watched" and is a form of spectacle (Lyon 2006b: 7, Mathiesen 1997: 222). Mathiesen demonstrates the significance of the spectacle in his article "The Viewer Society" as a form of power that works

alongside the Panopticon to help discipline the soul of its participants (Mathiesen 1997: 218). Mathiesen's article demonstrates that without the ability of the synopticon the behaviours of extreme resistance produced by the Panopticon may have been the only results.

Synopticism is "composed of the Greek word *syn* which stands for 'together' or 'at the same time', and *opticon*, which, again [like in the Panopticon], has to do with the visual" (Mathiesen 1997: 219). It is conceptualized to mean the many watching the few, and can be seen in all forms of media. Mathiesen was greatly puzzled as to why Foucault omitted a discussion of mass media in the analysis of panopticism because the "major media trends were certainly visible" during Foucault's investigation (1997: 221). The analysis and inclusion of mass media in Foucault's work "would necessarily in a basic way have changed his whole image of society as surveillance goes" (Mathiesen 1997: 219). Whereas Foucault argues that the spectacle was overthrown by the Panopticon as the new model of power, Mathiesen argues that both structures of watching (synopticism) and surveillance (panopticism) have grown synonymously in three parallel ways to "serve decisive control functions in modern society" (Mathiesen 1997: 219).

The first parallel is "the acceleration which synopticism as well as panopticism has shown in modern times, that is, during the period 1800-2000"; they have grown together and relatively at the same rate (Mathiesen 1997: 219). To illustrate how these structures have developed together, Mathiesen describes how the modern prison developed between 1750 and 1830, at the precise time that the mass press appeared (1997: 220). Over time, other systems developed that allowed both structures to follow, such as the television upon

which "hundreds of millions of people could see the few on stage" and CCTV surveillance cameras upon which a few could view the many (Mathiesen 1997: 221). That both "the panoptical surveillance structure and the media structure are parallel in that they are archaic, or 'ancient', as means or potential means of power" is the second parallel (Mathiesen 1997: 222). An example given by Mathiesen of a type of panoptic gaze was the system used by the Romans to enforce taxation. The Roman State "undertook such a large task as to tax, and thereby register, what was at the time 'all the world' in the archives of the state" (Mathiesen 1997: 222). Although this registration process failed, at the same time synopticism was being used by hierarchical leaders to leave visual and verbal impressions on masses of people. Foucault misses this main point "that the model of both systems go way back far beyond the 1700s, and that they have historical roots in central social and political institutions" (Mathiesen 1997: 222). Finally, the third parallel, and most important, is that "panopticism and synopticism have developed in intimate interaction, even fusion with each other" (Mathiesen 1997: 223). To demonstrate, Mathiesen illustrates how the military uses panoptic techniques as it "has always had a strict disciplinary hierarchy for providing possibilities for hidden surveillance from upper echelons of the system" (1997: 223). But it also uses synopticism as well in that military victories are highly visible (Mathiesen 1997: 223).

When both structures of panopticism and synopticism are combined together, a very strong model for power and control is brought forth. Mathiesen explains that "a vast amount of research shows that they [panoptical prisons] have only a marginal effect, in terms of controlled behaviour", as also illustrated by Lyon (Mathiesen 1997: 229). Hidden

apparatuses permit society's members to be aware of the constant gaze of surveillance; however, as Mathiesen states, "we remain, in our attitude, communists, left-oriented, or what have you, but adjust in terms of behaviour" (Mathiesen 1997: 229). People will still learn ways to be cautious or secretive to avoid observation or scrutiny. Synopticism, on the other hand, "through the modern mass media in general and television in particular, directs and controls the *consciousness*" (Mathiesen 1997: 230). It is able to successfully relate viewers to a paradigm, or understanding, of the world "because it is received in the context of a need - satisfies a need - for escape from the concrete misery of the world" (Mathiesen 1997: 230).

Taken together, both panoptic and synoptic structures silence citizens from raising critical questions of life and existence through its constant influence (Mathiesen 1997: 230). Surveillance "makes us silent about that which breaks fundamentally with the taken-for-granted because we are made afraid to break with it. Modern television, synopticon, makes us silent because we do not have anything to talk about that might initiate the break" (Mathiesen 1997: 230-231). Its convergence also works cyclically in that the more surveillance tapes are shown on the news, the more CCTV cameras are called for by its viewers to make their community safe. Resistance is difficult as it may "be silenced by the very panopticon or synopticon which we wish to resist" (Mathiesen 1997: 231).

Synopticism helps to explain how panoptic structures work to discipline and control society. Mathiesen's argument is significant because he does not omit the oppressive functions of the Panopticon, such as the discriminatory eye that "yields at least

part of its power" (Lyon 2006a: 46). Synopticism can be used to help explain why panoptic surveillance, through electronic technologies, is becoming so profound and accepted; so popular and enjoyable (Lyon 2006a: 47). However, several surveillance scholars strictly follow Foucault and do not focus on structures of the spectacle in their attempt to understand surveillance (Lyon 2006a: 50). On the other hand, there is also another group of scholars that focus solely on the synopticon. They are panoptic critics that believe "one literally *watches* the many [and] largely fail to note how synopticism and panopticism potentially work in concert" (Elmer 2004: 31). Thus, those that connect surveillance and spectacle seem to be very limited, and in some cases make the connection but fail to make reference to actual theory. To discuss this convergence, work from Elmer, Niedzviecki and Doyle will be used. These authors make reference to popular forms of watching that are relevant to modern society. The questions of trust that will be posed will also be more generalizable to contemporary society.

Watching and Being Watched

To gather information strict, intrusive surveillance methods may not be necessary, rather softer types of methods, such as anonymous surveys in malls, can collect abstracted data to stratify consumers (Elmer 2004: 38). "ATM machines, portions of the Web, and credit-card transactions" also collect abstracted consumer information; however, unlike the survey, this process is automatic (Elmer 2004: 38). In *Profiling Machines*, Elmer argues that pre-arranged categories gained through panoptic techniques can be used to facilitate synoptic viewing of television programs and increase purchasing habits as well (2004: 39).

For example, digital television "has begun to incorporate the collection of personal information within the act of viewing and recording programming" (Elmer 2004: 39). TiVo and other television recorders that collect information appeal to advertisers because the continuous tracking of a consumer's preferences allows companies to switch the recorded commercials to other ads that suit viewers habits and demographic profile (Elmer 2004: 40). Moreover, TiVo's Anonymous Viewing Information gives networks the power to recommend television shows to viewers because "the viewing data that TiVo collects also serves to link specific advertisements to a subset of consumers who have previously demonstrated through their viewing habits an affiliation with the product or service" (Elmer 2004: 40). "In short, TiVo reminds us that what we watch (synoptically) is becoming even more select (via panoptic process) - that viewers are getting exceptionally familiar, 'more of the same' programming" (Elmer 2004: 40). This limits access to difference and may act to silence the viewer from criticism that could potentially develop (Elmer 2004: 40). Elmer ultimately argues that consumers may not be entirely disciplined by the Panopticon, rather "they are both *rewarded* with a preset familiar world of images and commodities, and *punished* by having to work at finding different and unfamiliar commodities if they attempt to opt-out" (Elmer 2004: 49). In the end, people are pushed into silence and conformity through both structures working together to make resistance a difficult task. The familiarity that is produced and extended by watching brings forth issues of trust. Watching similar television shows may be a common ground for strangers to relate. Can the familiarity in television programs bring about relations between people that actually build trust and more connections?

Niedzviecki, in his book *The Peep Diaries,* describes aspects of the viewer society through his outlook on what he terms peep culture. Prior to electronic technologies, Niedzviecki states, "we were taught that spying, peering, and peeking in on people, is no way of behaving" (Niedzviecki 2009: 18). The parable of Peeping Tom has made this lesson clear in that when Lady Godiva had ordered all the townspeople to hide their eyes as she rode through the town naked, Tom was struck dead or blind upon failing to do so (Niedzviecki 2009: 18). This sent the message that "creeps who peep get what they deserve" (Niedzviecki 2009: 19). However, with the popularity of "urgent, expedited revelations regarding the problems of celebrities" spread throughout television, magazines and newspapers there has been a change in the lesson; we are learning that it is okay to participate in peep culture - "an entertainment derived from peeping into the lives of others" (Niedzviecki 2009: 6). In fact, programs such as blogs, Facebook and Twitter permit the sharing of excessive personal information, making it so that "[w]e don't need to wait for the next celebrity breakdown or pregnancy to have our fun" (Niedzviecki 2009: 6). The attraction of potentially having an audience, fan club or online community may be reason enough for people to continually share too much personal information online.

This desire to watch and be watched in Niedzviecki's peep culture reflects the convergence of synopticism and panopticism. Synopticism reflects how people share information online, "everything from sober family gatherings to drunken frat parties to kinky amateur sex parties" to demonstrate that they have something valuable to share and are worth watching (Niedzviecki 2009: 10). While this type of detailed information is revealed, the functions of panopticism work in the background to "assign a price tag to

every secret, scandal and crime, every seemingly commonplace domestic moment" (Niedzviecki 2009: 20). Niedzviecki states that in using these tools people are trying to regain those "things that were once provided by community", such as the "essential recognition of our humanness, intrinsic acknowledgment that we exist", which we have lost in our highly organized society (2009: 27). It is done "to meet a need that our society seems no longer to fulfill" - to satisfy and repair the disconnect between neighbours and communities (Niedzviecki 2009: 26). Research has found that online communication actually works to provide something like community for some. In using online tools, such as blogs, people reported "feeling less isolated and more part of a community, as well as happier with their friendships both online and off" (Niedzviecki 2009: 29). However, this online community and attention is the "responsibility of corporations, governments and bureaucrats"; those with "economic and political power, that systematically and increasingly defines the criteria or frames of reference for the information which is to be stored, which is to be available, and which subsequently may be selected, combined and recombined" (Niedzviecki 2009: 27, Mathiesen 1997: 225). "As a result, despite the seeming appearance of rampant individualism in our society [that comes with the belief that the internet is an anonymous realm of free space], we are actually more observed, managed, categorized, and analyzed, and ultimately more conformist than ever" (Niedzviecki 2009: 27). Online tools may be a way to create communities, but can the technology replicate the trust and strong ties that were once built in traditional communities? Can online communities really be backed by trust when there is no face to face interaction?

Building online communities, it has also been argued, reinforces and encourages thought patterns and practices of individuals; to keep them in line with all that is familiar (Niedzviecki 2009: 31). Both synoptic and panoptic structures work together in this case to silence people as both voyeurs and sharers conjointly act "together in cybernetic harmony, each one encouraging the other, neither stopping to think about what's happening and why" (Niedzviecki 2009: 19). As in the situation of watching television, critical thoughts about possible negative outcomes are left out and not discussed. And when Internet users get caught up in the virtual experience they begin to forget about the existence of the social order offline, one which still holds traditional values and where there is "always the chance that people will see you [a blogger, or Facebook user] as damaged goods and decide they don't want to have anything to do with what you're selling" (Niedzviecki 2009: 55). The new 'order' of society is confusing and the majority of people may not know what to make of it. How do online users forget about the offline social order that can use public profiles or online videos to judge trustworthiness? Why do they put themselves at risk?

Those who do not wish to share information online can support panoptic and synoptic technologies through watching news reports or television shows that depict crime. Doyle argues in *Arresting Images* how the media can provide a spectacle that creates an emotionally charged audience who may work together to influence or change an institution (Doyle 2003: 152). Specifically, he concentrates on crime and policing and how its injection in television can create retributive criminal justice (Doyle 2003: 152). Surveillance footage reproduced on news stations is a type of promotional footage "because it often promotes the problem of crime and the solution of 'law and order' in

general, or in particular the use of surveillance cameras themselves as a solution to crime"(Doyle 2003: 69). This footage creates a "new institutional role for the audience as a participant in surveillance" (Doyle 2003: 66). Audience members see the benefits of panoptic technology and engage in the role of identifying and reporting suspects. This impacts the justice system in that emotionally charged viewers can intensify formal punishment and pre-empt "the accused's right to a fair trial, [by creating a] 'trial by media'" (Doyle 2003: 69). An example of enhanced punishment through media is the shocking and widely broadcasted media depiction capturing a nanny slapping an infant in her care. The punishment given was beyond necessary because the public outcry ensured that "the ex-nanny [would] probably never outlive the incident, said her lawyer: 'It was like taking a sledgehammer to an ant'" (Doyle 2003: 69).

These images dramatically reproduced for the purposes of entertaining, play upon the theory of synopticism while still encouraging panopticism. Promotional footage ensures the continual use of panoptic technology and can manipulate viewers by playing on their fears of crime. The structure of the synopticon in this instance works to communicate to the viewers the dangers of street crimes and how the justice system fails to aptly punish certain broadcasted crimes (Doyle 2003: 71). Although it may seem as though television has a fair portrayal of political, high class crimes as well as low class, street crimes, the synopticon still works to benefit major companies and government organizations (Doyle 2003: 71). To illustrate this, class differences are apparent in televised footage in that the "surveillance produced by the interaction of cameras, authorities, and broadcast television will be a selective one that will tend to work to the advantage of police and other dominant

institutions and groups, and work against the less powerful" (Doyle 2003: 71). Bias exists in surveillance footage as well because public surveillance cameras tend to be present in poorer areas, and surveillance operators, who "have the power to interpret the images – who produce the authorized definition of the situation – are the ones who hold the upper hand," focus on stereotyped groups (Doyle 2003: 71-72). Also, these television shows, such as *Cops,* "tend to underrepresent African Americans and Hispanics and overrepresent whites as police officers, while over representing minorities and under representing whites as criminals" (Doyle 2003: 52). Clearly these features work to reproduce inequality, only on a mass level because so many people have the opportunity to watch without critically thinking (Doyle 2003: 71).

What is vital in Doyle's investigation is not just that television represents crime in a way that fosters "more punitive public attitudes towards crime", and that these, in turn, directly influence the justice system in a variety of ways, but that surveillance communicates to the entire population (Doyle 2003: 147). Through its screening in the media, surveillance has expanded its reach, "has also become more literally visual again", and sends messages to the public (Doyle 2003: 154). It communicates:

> That crime is everywhere; that others among us are not to be trusted, especially those who are visibly different; that technology rather than community is our safeguard; and that the answer is to surreptitiously monitor all others and report them to authorities, specifically the police, who are the only ones authorized to act in order to deal with the crime problem. (Doyle 2003: 154)

Clearly this implies that television can communicate that certain kinds of individuals in society are untrustworthy. However, television can also communicate that other areas in society, such as the judicial system, also cannot be trusted because they fail to provide

satisfying results, such as accurate punishments to criminals. In this way, a question of trust can be posed to television as a whole. Can television communicate distrust in all members of society? Conversely, is there any way for television to generate trust in society?

The Synopticon and Trust

The synopticon and the Panopticon work hand in hand to de-stigmatize close surveillance (Lyon 2006b: 7). Through watching, society has been taught that being seen can be desirable which reduces the extreme behaviours of resistance that an actual case of the Panopticon can produce. Working together, the Panopticon and synopticon have the potential to control the mind and the body, making individuals silent about critical ideas or change. New technologies that have developed can be understood as either creating or destroying trust because they can be used to make or limit connections between individuals. For example, the Internet can be used to initiate interactions between strangers, but are these interactions or online groups really supported by trust? Also, television can possibly destroy trust by communicating to the public that no one is to be trusted. But television has the potential to create relationships because of the shared familiarity of programs. Since these technologies can affect large masses of individuals a conceptualization of trust from the discipline of sociology will be used.

Sociology and Trust

Trust is vital in the functioning of society. Without it society would fall apart because "very few relationships are based entirely upon what is known with certainty about another person, and very few relationships would endure if trust were not as strong, or

stronger than, rational proof or personal observation" (Simmel as quoted in Misztal 1996: 50). There is a need for trust in society because not everything can be known about systems, individuals, companies or motivations. Without it "only very simple forms of human cooperation which can be transacted on the spot are possible, and even individual action is much too sensitive to disruption to be capable of being planned, without trust, beyond the immediately assured moment" (Luhmann 1979: 88). It is this idea of the significance of trust that is important to sociology as "[s]ocial theories tend to conceive of trust by pointing to the range of benefits that trust provides" (Misztal 1996: 12). Trust can be viewed as a public good which is essential for the economy, effective problem solving, the formation of autonomy, "fostering democratic values and as the basis for sustaining republican society or civic community" (Misztal 1996: 13). Traditionally, "the valuable public good, such as trust, was supplied by common tradition, community and the Church" (Misztal 1996: 6). However, with the diminishment of these foundations for trust, Misztal questions "[w]hat are the sources of trust now?" (1996: 6). The social sciences "have attempted to study [trust], or at least register its presence, but without a great deal of effort being devoted to its conceptualization" (Misztal 1996: 13). The definition of trust will be taken from Misztal where "to trust is to believe that the results of somebody's intended action will be appropriate from our point of view" (Misztal 1996: 24). However, questions of trust revolve around the building or backing of trust by elements such as electronic mediums or familiarity, which cannot be answered by this definition. Instead these elements will be looked at to see if they produce the functions of trust. For example, does television create meaningful interactions, effective problem solving, participation in

community or encourage the formation of autonomy? Can they be a source for trust? If they are producing the functions of trust, then trust has been built. To demonstrate whether the elements present in the synopticon generate or destroy trust, the work of Putnam, Tilly, Niedzveicki and Misztal will be examined.

One of Putnam's main concerns in his book *Bowling Alone* is that of social trust, "*not* trust in government or other institutions" (Putnam 2001: 137). This is because "trust in other people is logically quite different from trust in institutions and political authorities" as a person who does not trust the provincial government will still easily trust a neighbour (Putnam 2001: 137). In Putnam's examination, he discusses two specific types of trust: thin and thick trust. "Trust embedded in personal relations that are strong, frequent and nested in wider social networks" is thick; whereas "on the other hand, trust in 'the generalized other,' like your new acquaintance from the coffee shop, also nests implicitly on some background of shared social expectations of reciprocity" where reciprocity is the expectation of a return sometime in the future out of respect for the initial exchange (Putnam 2001: 136). Putnam argues that thin trust is more useful than thick trust "because it extends the radius of trust beyond the rosters of people whom we can know personally" (2001: 136). It is also useful in that it allows potential to build deeper relations by giving "most people - even those whom one does not know from direct experience - the benefit of the doubt" (Putnam 2001: 136). Having trust in fellow citizens functions to benefit society in that people will "volunteer more often, contribute more to charity, participate more often in politics and community organizations [...] and display many other forms of civic virtue" (Putnam 2001: 137).

After looking at several years of American surveys on beliefs which question whether most people are trusted or that they cannot be too careful around others, Putnam finds that "every year fewer and fewer of us aver that 'most people can be trusted'" (Putnam 2001: 140). Even younger generations are following this pattern of belief, "telling us that in their experience most people really *aren't* trustworthy" (Putnam 2001: 142). As a result, Putnam suggests that "perhaps thick trust - confidence in personal friends - is as strong as ever" but that consequently, thin trust - the "crucial emollient for large complex societies like ours - is becoming rarer" (2001: 145). Being a reflection of the inner self, this can play a role in people's attitudes or behaviours in actual society, where social distrust may reflect "personal cynicism, paranoia, and even projections of one's own dishonest inclinations" (Putnam 2001: 138). This may also play a role in the call for enhanced law enforcement as "if the handshake is no longer binding and reassuring, perhaps the notarized contract, the disposition, and the subpoena will work almost as well" (Putnam 2001: 145). With trust, communication between individuals can easily initiate and build a starting point for more deeper and meaningful relations to develop. Since there is a lack of generalized trust, people may find solace in things such as watching the same television programs and communicating electronically with other "fans". Can those elements of the synopticon - television watching, familiarity and online communities - reproduce or build the foundations for trust to provide its various beneficial functions?

Television and Trust Building

Television does not appear to foster any kind of trust. Rather, technology and mass

media contributed to the decline of social interaction that can damage trust. Putnam argues that "news and entertainment have become increasingly individualized" where "[n]o longer must we coordinate our tastes and timing of others in order to enjoy the rarest culture or the most esoteric information" (2001: 216). With the average American estimated at watching "roughly four hours per day" and the "single most important consequence of the television revolution" being the idea that viewers now enjoy being at home, television can have the effect of cutting into time for social interactions. Viewing is a form of leisure that is often privatized, and "just as television privatizes our leisure time, it also privatizes our civic activity, dampening our interactions with one another even more than it dampens individual political activity" (Putnam 2001: 229). It can have an effect on relationships in that "more time for TV means less time for social life", leaving less opportunities to successfully develop thin trust (Putnam 2001: 238). A way that television can potentially encourage relationships and civic participation may be watching the news as "TV news viewing is positively associated with civic involvement" (2001: 220). However, with "[m]ost of the time, energy and creativity of electronic media [...] devoted not to news, but to entertainment" participation in civic activities decreases (Putnam 2001: 221). Altogether, as "[w]atching TV, videos, and computer windows onto cyberspace is ever more common [and sharing] communal activities is ever less [common]" television decreases the amount of time available to create strong ties or deeper relations with others (Putnam 2001: 245).

The familiarity that Elmer touches on may seem like some ground that can build relations between people. This is partially because it is possible for those watching to feel

as if they do have a connection through television. Television personalities can offer "false sense of companionship, [that make] people *feel* intimate, informed, clever, busy and important. The result is a kind of 'remote-control politics,' in which we as viewers *feel* engaged with our community without the effort of actually *being* engaged" (Putnam 2001: 242). Feeling as though they are engaged, people may not participate in actual events. This may act to stop actual civic participation and any chance at developing thin trust. Familiarity can also generate connections between individuals because discussions can stem from popular television shows between coworkers, acquaintances and even strangers. However, this connection does not necessarily demonstrate any meaningful interaction or trust. That is, although "[t]he bonds nurtured by these common experiences are psychologically compelling, [they] are generally not sociologically compelling, in the sense of leading to action" (Putnam 2001: 244). Like "two kids in a sandbox, each playing with a toy and not interacting with each other", "public spectacles leave us at that arrested stage of development, rarely moving beyond parallel attentiveness to the same external stimulus" (Putnam 2001: 244). Television does not lead to action beyond its goals of entertaining and keeping eyes glued to the screen. Any effective ideas that could occur are hindered or geared towards the ideals communicated by the media. Doyle's argument acts to further demonstrate how television viewing can destroy chances at thin trust because of its messages to the public. However, this message extends to government and other powerful institutions as well, furthering distrust. Although it may seem as though audiences are empowered because of this chance to scrutinize the powerful, "[w]hat becomes news and consequently what we 'view' is selected for us by a smaller number of

editors and procedures according to institutionally developed criteria" (Innes 1999: 273). Ultimately, the media has "its own set of guiding principles and objectives" that are followed and supported by a large audience who view these programs (Innes 1999: 273). Thoughts of action are geared towards these objectives of media and the synopticon works to stop any type of critical thought.

Online Communities and a False Sense of Trust

A response to online communities and whether they are backed by actual trust or can produce trust may be met by Tilly's discussion of trust networks. He notes that "[a]lthough some trust relationships remain purely dyadic for the most part they operate within larger networks of similar relationships" (Tilly 2005: 12). Online communities may be built by familiar thought patterns or tastes between members; however this does not fulfill the idea of a trust network. Trust networks are defined as "[r]amified interpersonal connections consisting of mainly strong ties, within which people set valued, consequential, long-term resources and enterprises at risk to the malfeasance, mistakes or failures of others" (Tilly 2005: 14). Online communities, where individuals connect with anonymous strangers, may fall under "single-stranded networks containing few triads and sustaining little intimacy among their nodes [which] rarely or never become trust networks" (Tilly 2005: 13). This is partially due to the fact that online users can choose to leave communities guilt free and at no risk because there is no obligation to stay. Though having similar thought patterns, making connections in the virtual world are not likely to persist in reality and thus the strong ties that are formed by trust are not created online.

Take, for example, social movements where members take collective action with other members who "have strong ideas about what is wrong in the world" (Henslin, Glenday, Duffy and Pupo 2004: 435). Activists who "form international alliances rely increasingly on electronic communication, most recently the internet and portable mobile devices", but they fail by "reducing the influence of ideology on personal involvement in social movements" (Tilly 2005: 155, 156). This creates "loosely structured networks, rather than the relatively dense networks of earlier social movements" (Tilly 2005: 156). As "social movements [become] increasingly vulnerable to problems of coordination, control and commitment", it seems that the Internet and online communities cannot create the same, meaningful or committed bonds that strong social ties could (Tilly 2005: 156). The implication is that if trust was developed, successful social movements would be produced and problems would likely be electrically solved and real social change initiated.

Two factors can be used to explain why online users may forget about the offline social order and why they participate in risky behaviours. The first factor is because traditional communities, in which "people are typically available to each other in person", and where "the trust emanating from 'looking each other in the eye', from the deal sealed with the handshake and so on" is what held social relationships together, have been lost (Lyon 2001: 15, 16). Through this, people have lost the feeling that they are "ordinary and normal and deserving of everyday human interaction" (Niedzveicki 2009: 27). The second factor is related to the first: since community has been lost, so too are the structures to educate newer generations that "tell us who we are, whom we should trust, [and] how we should live" (Niedzviecki 2009: 147). Facing the "ongoing process of globalization [...]

modern industrial nations are being forced to redefine and articulate new collective values and aspirations" (Misztal 1996: 4). However, online communities cannot build these values. Rather, in trying to achieve recognition that used to come with community, users participate in rambunctious behaviours as some "actively seek out the trappings of shame as a way to set [them] apart from the anonymous, easily ignored mass" (Niedzviecki 2009: 147). These acts almost replicate the behaviours of the panoptic prisoners who would do anything to resist the gaze. Whether these acts or beliefs expressed on the Internet are true or not, they can have real world consequences as "[a]s the various college students who have been themselves denied jobs and even jailed based on their public profiles can attest" (Niedzviecki 2009: 269).

The online virtual world is not a space where a "redefinition of rules [could occur] by which [we] structure [our] existence" (Misztal 1996: 4). This is because online communities and programs are "inextricably connected to forces of bureaucracy, capitalism, and law and order" that keep society functioning in appropriate ways (Niedzviecki 2009: 269). It is not a reliable place to look to for social solidarity, cooperation and consensus because of this connection. It further damages the potential to create trust in society because "if people *could* know and trust each other in an intrinsic communal way, could see us all for who we really are, we would not have seen this rise of Peep culture in the first place" (Niedzviecki 2009: 269). The Internet provides an outlet for people to display untrustworthy behaviour which can further distrust in some members of society. Trust and meaningful social relations have been lost that could function to prevent extreme behaviours. Instead, there seems to be a reliance on other mechanisms to maintain

social order.

The Synopticon, Sociology and Trust

Trust in sociology is understood as providing a range of benefits to society. However, the technology that is becoming more commonly used and watched does not provide ample opportunity to build trust that provides beneficial functions, such as meaningful social interactions, effective ideas for problem solving, strong ties, preventing harm or maintaining the social order. It can, in fact, have the opposite effect and destroy the thin trust that could be used to create communities. As stated, watching television stops interactions necessary to build trust, while its programs can either cause distrust or hinder conversations that may be grounds for critical thought or social change. Online communities fail to truly provide trust networks as attempting to gather together offline demonstrates a lack of commitment. They also fail to create the community that is longed for, and, in its absence, individuals act in shameful and distrustful ways to gain attention and in return, suffer institutional consequences by law or bureaucracy. The Internet cannot facilitate the function of trust that would create "patterns of normalcy" and values (Misztal 1996: 4). Altogether, it shows that these media cannot supply or serve as sources for interactions that are strong enough to foster trust in society. Reliance is placed upon other systems, such as law or strict standards, to uphold the social order where trust once functioned. As a result, we may be demanding more surveillance to provide us with safety in our own neighbourhoods, eroding the potential for social trust.

Chapter 3

(In)Security and Trust

Everyday we are met with a challenge of security that requires us to prove our identity and legibility by providing acceptable documents. Security is the fact or state of being secure, that includes taking measures to prevent illegal entry, sabotage, or escape. The task of security procedures and the reason why they are in service is to produce a state or feeling of being safe and protected. And increasingly surveillance is used as a means to establish this publicly. However, it has been argued that security seems to be less and less concerned about "reacting to, controlling or prosecuting crime", the more conventional viewpoints of policing, and more concerned about "addressing the conditions precedent to it" (Aas, Gundhus and Lomell 2009: 2). This means that security is more concerned about predictability that can be accomplished using surveillance technology to help identify or determine risk. The problem with surveillance is that the technology alone cannot determine risks, rather common techniques of profiling, interpreting, sorting, and classifying are used with the technology; techniques that are not always neutral or free of biases. Surveillance can cause errors that are detrimental not only to those people who are unaware that they are its targets, but can cause "critical issues [of] trust and suspicion" in specific groups or the general public (Aas, Gundhus and Lomell 2009: 1). The use of an immense amount of security technology can raise questions about where trust from society's members is placed; is it placed more in security technology and less in each other? And also raise questions about what happens to the trust when the technology fails. In this chapter security technologies will be analyzed as well as different perspectives on

the subject. A discussion will follow on the problems of security technology by using theories from Aas, Gunhus and Lomell, Andrejevic, Neyland, and Bigo. Questions of trust will be added and examined from the perspective of social psychology.

Security Technology: Support and Criticisms

Surveillance practices for security can range from "high- to relatively low-tech", are comprised of virtual and concrete technologies, and "their deployment ranges from expert to the amateur" (Zedner 2009: 257). Security technologies include: identification technology that "focus on personal details for purposes of entitlement, access and policing" such as licenses and social security cards, closed circuit television (CCTV) cameras, alarm systems, the new body scanners at the airport; virtually any surveillance technology can be used to monitor for the purpose of safety (Lyon 2009: 142). They are used to recognize risks and establish identities for previously mundane objects that are altered to be seen as dangerous and needing security, such as "water bottles or other liquid containers [that] have at times shifted from the ordinary, comfortable and everyday into categories of suspicion" (Neyland 2009: 21). Furthermore, CCTV surveillance cameras are supervised by operators who are "also *workers*, subjected not only to the same capitalist regimes as any other labourer in late modernity but also to an emotive duress produced by the very technologies which earn them their living" (Smith 2009: 126). Consequently, they are "predominantly *choosing*, as a result of their subjectivities and the workplace culture in which they are embedded, to target and associate criminality to the young, working class males, ethnic minority populations, sub-cultural groups and particular forms of mobility"

(Smith 2009: 129). All of these technological security practices can be "linked to power, governance and risk management" and have been shown to have ulterior goals other than public safety (Smith 2009: 133). This can be seen, for example, with CCTV in public spaces in which "the technology's rapid deployment is tied to strategic spatial-management programmes and political-economic policies as it is primarily concerned with securing predictability and controlling people and movement" (Smith 2009: 133). It is important to realize that although there is a common belief that many of these security technologies have come into play mostly after 9/11, "the practice of watching others in order to detect inappropriate behavior or to avert danger and risk is nothing new" (Lyon 2003: 1). 9/11 enabled heightened security surveillance practices in the United States, which spread to other countries such as Canada and Britain. Rather than being generated for safety out of the interests of others, it has been argued that "many well-meaning initiatives since September 11 both fall short of promises made for them and at the same time create new problems that will limit freedom of movement and self-determination, and augment the power and the accountability of governments and corporations [...] 9/11 is pushing the pendulum from care to control" (Lyon 2003: 11).

The debate surrounding "new technologies and their security effects has been polarised", with critics tending "to portray the introduction of new technologies as heralding the advent of a dystopian and totalitarian society", and supporters celebrating the new technology "as 'silver bullets', offering the possibility of radically reduced levels of crime and more efficient and effective policing" (Aas, Gunhus and Lomell 2009: 3). Supporters often view security technologies as an effective method to reduce threats of

violence and ensure community safety. This is partly due to the ostensible technical neutrality as the technology "appears as reasonable and not subjected to classic racism" (Bigo 2006: 60). It may also be viewed as a solution to demands for equality because it has the ability to bring about justice, as surveillance through "identifying citizens may also be the means of ensuring their entitlements and their rights", even in places such as interrogation rooms (Lyon 2009: 44). Furthermore, a crisis may lend support to the idea of a technical solution. For example, "[i]n the immediate aftermath of September 11, few people challenged the idea that the sovereignty and integrity of the body of the US nation were at stake [...] instead they participated in the creation of a new wave of patriotism, an appeal to be more protected and a will to revenge" (Bigo 2006: 52). However, the problem with such support for security technology is that it can produce an over-reliance on technology to solve security problems that undermine other solutions such as "developing reasonable antiterrorist policies" (Bigo 2006: 60). It is clear that the idea of maximum or guaranteed security is "simply unattainable" and a reliance on security technology to provide this "carries with it some avoidable problems" that become evident when the technology fails to sustain the security that it promises (Lyon 2003: 16). Problems with security technologies include the erosion of social trust through forms of insecurity and suspicion, its potential to be overly intrusive, as well as its ability to cause "conditions that are not merely disagreeable, but unjust and unfree" (Lyon 2003: 6).

Problems with Security Technology

"[D]espite avowedly being dedicated to the endgame of security," surveillance

technology may erode social trust in the way that it "construct[s] new dimensions of insecurity" (Zedner 2009: 265). Aas et al. use the term "(in)security" to depict how the two opposed concepts are deeply intertwined with each other and demonstrate how security technology inherently produces feelings of insecurity. Insecurity can be defined as feeling unsafe or vulnerable, feelings that can become instilled through making something that was once considered safe more dangerous. This can occur, for example, where surveillance cameras are set up in areas that are not considered particularly dangerous such as classrooms and elevators. In doing this new attitudes may develop regarding places, people and environments that are surveilled. This may result in "social relations [that become] marked by distrust and uncertainty, particularly with regard to certain social groups defined [or targeted] as security threats" (Aas, Gunhus and Lomell 2009: 2). 9/11 has increased these feelings of anxiety because the threat became ambiguous as the "novel element of the so-called war on terror was that the enemy's weaponry took the familiar form of passenger jets, cars, computer code, and even the daily mail" (Andrejevic 2007: 168). When this happens there is a "need for verification technologies [that] multiplies along with responsibility of individuals for monitoring a climate of proliferating risk" (Andrejevic 2007: 168). Security technologies may be viewed as ways to maintain safety, but they also may cause issues of distrust in others by generating feelings of suspicion. This raises questions about the level of trust between members of society and where that trust goes when too much security technology is put in place.

Suspicion is a general lack of trust in a person or a lack of certainty. It can be manufactured by security technologies and is another of its problems that can lead to the

erosion of social trust. The effects of 9/11 are a perfect example to demonstrate how surveillance creates suspicion. After the attacks, the United States heightened domestic security practices, enlarging the culture or climate of suspicion that "potentially taints all reputations and makes surveill*ors* of us all" (Lyon 2003: 10). Citizens then began to participate in surveillance procedures, through encouragement by government departments such as the Department of Homeland Security, by looking out for questionable behaviour or unusual packages; elements of terrorist activities that security experts have defined as possible threats. The problem with terror is that the definitions given by these experts are unclear and left mostly to interpretation. For example, a British intelligence agency describes a letter bomb as "probably [having] received fairly rough handling in the post and so is unlikely to detonate through being moved, but any attempt at opening it may set it off" (Neyland 2009: 27). This identification includes vague detail and use the language of uncertainty that could make any letter seem suspicious. A more substantial problem ensues when this vagueness and uncertainty extends to terrorist descriptions where "[t]he foreigner [who is now stereotyped as the terrorist] is no longer the non citizen, he is the one with the strange, bizarre and slightly deviant abnormal behaviour, or the opposite, having such normal behaviour that it seems suspicious" (Bigo 2006: 60). Trust may not be so easily given to strangers with such general descriptions of danger and the responsibility of safety may be given to security experts as procedures to manage the threat are followed which suggests "who should be taking responsibility for managing the risk of letter bombs" or suspicious people (Neyland 2009: 26). Given the circulation of uncertain elements, questions about whether security procedures are trusted or ignored may be raised.

Stereotypes can easily be transmitted into feelings of suspicion, especially after 9/11 which led to targeting "along 'racial' lines, focusing on 'Arab' populations in particular" as categories of suspicion (Lyon 2003: 31). With surveillance technology enhancing the amount and extent of observation of these groups, more and more stereotyped groups may face unjust conditions thanks to a technique called profiling. Profiling is used by security to be able to "anticipate before the act, who is going to commit an offence and what their actions will be in the future" (Bigo 2006: 62). The process is similar to the profiling of customers by corporations that use patterns in trends and behaviours to anticipate future purchases. Profiling can be dangerous because those who have been "judged to be a sign of potential danger" are put under a more serious surveillance regime (Bigo 2006: 59). This is faced mostly by those people "constructed as a specific 'minority', [or] 'abnormal' group, [because they are viewed as] a group with virtually violent behaviour, even if this behaviour has never been actualized" (Bigo 2006: 61). The consequences of improper interpretation can be detrimental as "effective controls and coercive restrictions of freedom are concentrated on specific targets" (Bigo 2006: 63). Some of these controls of minorities were in place long before 9/11, but 9/11 has acted to construct these individuals "as 'invisible and powerful enemies in networks'", justifying "the profiling of certain people's potential behaviour, especially if they are [considered] 'on the move'" (Bigo 2006: 63). Using profiling and security technologies to fabricate "body identification as a sign of a predictable pattern of behaviour" fails because it is based on assumptions, yet it has the power to exclude its targets from everyday activities and life chances (Bigo 2006: 63). How does the targeting of stereotyped groups affect their level of

trust in society and government?

Another failure of security technology is its creation of a state of perpetual fear that may only, seemingly, be resisted by being constantly prepared. After 9/11, the Department of Homeland Security (DHS) was developed in the United States to secure the country from environmental disasters and preserve freedoms (Homeland Security Website). Included in its mission to secure the homeland was a section on terrorism which "is portrayed as a form of second nature: an additional uncontrollable force in the world, just as independent of national policy as a tsunami or earthquake" (Andrejevic 2007: 182). To protect from this threat, the DHS encouraged U.S. citizens "to take responsibility for preparing for catastrophes," and advised citizens to participate "in an ongoing homeland security surveillance program against terror" (Andrejevic 2007: 164). Andrejevic notes that "[r]ather than conserving, citizens are urged to consume and seek out investment opportunities that disconcertingly capitalize on the terrorist threat" (2007: 164). In the DHS's attempt to get citizens acquiring "the necessary equipment and training to take duties offloaded on them by the state", individuals began to take "on the duties of being a good consumer" and invested in security technologies such as encoding devices, metal detectors and even duck tape (Andrejevic 2007: 165, 183). Citizens were also to assume their role in the war on terror by taking responsibility "as they [went] about their daily lives at work, at home and at school" (Andrejevic 2007: 173). Consuming security technologies for everyday activities not only reminds people of "the failings of the government bureaucracies in securing the nation against terrorists" but also echoes the idea that citizens need to protect themselves by following the advice distributed by these same government

bureaucracies (Andrejevic 2007: 165). Safety and protection is no longer only in the hands of the state, but is also, and more importantly, in the hands of citizens who can choose to consume or participate in safe practices. This definitely raises questions about the trust society places in the government. If the technologies used by the security departments of the government are not working, then how is society able to place trust in the government? Also, how can society place trust in safety equipment that even when used by professionals do not work?

Although the point of taking responsibility and being prepared is to abolish fear, the account of preparation "entails not an abolition of fear but a stance of perpetual anxious diligence": a state that is good for security businesses (Andrejevic 2007: 167). Andrejevic argues in the midst of 9/11 what has emerged is "the individualization of warfare and [...] the individualization of defense" (2007: 182). The message to the people in the United States was to be prepared, which meant anything from buying dust masks to the Executive Chute, "a parachute for those who work in skyscrapers" (Andrejevic 2007: 183). Security industries that are privatized realize that "anxiety is especially productive, and risk can be leveraged for profit" which means that a state of perpetual fear, conveniently created through the generalized risk that was provided by terrorism, is good for business (Andrejevic 2007: 184). This was not only realized after 9/11, but had been realized prior to the event and can be seen in the invention of previous security technologies. The sports utility vehicle (SUV), for example, was advertised as a safety vehicle, but turned out to offer less protection to other vehicles on the road as it actually promotes aggressive driving and reduces visibility (Zedner 2009: 268). Thus, the "selling of the SUV as a mobile

security environment might better be read as a marketing ploy that plays on people's insecurities" (Zedner 2009: 268). Again, this causes insecurity and does not necessarily obliterate fears. The problem with the privatization of security industry is that it profits from fear and anxiety. Will trust continually be put in the hands of the technology that is supposed to create safety? Or will individuals come to the realization that buying into security creates more insecurity?

Security Technology and Trust

Despite all of the problems and failures of technology, people are still consuming surveillance technology; as Andrejevic makes clear, making America safe is a 215 billion dollar a year business (2007: 165). Also, security procedures are still in service with little resistance from individuals as after a while, "these technologies seem so banal (such as ID checks in many countries, military with heavy armaments in public places, and biometric identifiers) that nobody (including judges) asks for their legitimacy and their efficiency after a certain period of time" (Bigo 2006: 49). With both monetary support and acceptance it seems as though the technology and its services are trusted. However, social trust is affected in the way that a climate of suspicion has expanded, insecurity has risen and the unjust conditions have grown from intrusive surveillance techniques. How does the insecurity of security technology affect society's trust in government and between its members? Can too much security act to destroy trust? Or can people become accustomed to its presence and continue to trust others? How do security techniques and technology affect the levels of trust between stereotyped groups, government and society? To attempt

to answer these questions an understanding of trust will be taken from the discipline of social psychology.

Social Psychology and Trust

Within the frame of social psychology, the concept and use of trust is limited, but significant when applied to security technology. Social psychology "examines the influence of social processes in the way people think, feel and behave" (Westen 2002: 593). It can be applied to the area of security because the "expert-labelled social problems as types of 'risks', social behaviours as 'risky' or types of people at 'risk' are all held to comply with efforts to govern societies according to the principle that individuals" need to take responsibility for the security of their families and themselves (Wilkinson 2006: 36). Individual responsibility for security implies a type of lateral surveillance which "[r]ather than strengthening communities and building partnerships, [...] destroys trust and produces interpassitivity" (Chan 2008: 225). Privatization of security also introduces a new portrayal of the risk society as comprised of "an aggregate of individuals all sharing in common cultural experiences of risk and all bearing personal responsibility for their fates" (Wilkinson 2006: 36). With risk and security being made into more of an individual problem propelled by privatization and government encouragement, social psychology becomes a useful discipline to examine trust because it looks at individual choices of trust and distrust. It uses social settings and situations as important factors in the reasoning for an individual's decision to trust or distrust. The definition that will be taken from this discipline will be from Rotter's work in which trust is a "generalized expectancy held by an

individual that the word, promise, oral or written statement of another individual or group can be relied on" (Rotter 1971: 444). To look at trust in security, works from Rotter, Hardin, Yamagishi, Mirowsky and Ross, and Glover will be examined.

Rotter: Expectancies and Trust

In psychology, "most argue that we learn to trust" based on the teachings of parents to infants (Cook, Hardin and Levi 2005: 22). Similarly, "Rotter and other social psychologists focus on the capacity for trust as learned from experience" (Cook, Hardin and Levi 2005: 23). Though Rotter's work is older, it has been influential to developing new strategies of trust measurement and understanding. As the modern world changes and grows with more and more surveillance, Rotter's work becomes meaningful because "the notion that the major portion of human social behaviour is learned or modifiable" is applied (Rotter 1972: 4). He bases his work from social learning theory, which "was developed as an attempt to account for human behaviour in relatively complex social situations" (Rotter 1972: 1). Situations determine the trusting or distrusting response because "expectancies generalize along lines of perceived similarity, relatively stable modes of responding develop, and a learned basis for a theory of personality is developed" (Rotter 1971: 445). Rotter preferred to look at situations because "common sense [would be] based on an understanding of a culture rather than reading from an instrument" (Rotter 1972: 13). Similar to most literature on trust, Rotter agrees that there are "enormous personal costs of excessive distrust" (Rotter 1980: 1).With an increase of distrust in society that he argues is present in the 1970s and 1980s, Rotter states that "the attempt to

decelerate what appears to be increasing distrust and to build a society in which people trust each other may, in itself, demand changes in the behaviors of individuals and groups that constitute positive social change" (Rotter 1971: 444). This means that changes must be made on a large scale. Expectancies of distrust can change only when people work together to create generalized expectancies of trust because "expectancies in each situation are determined not only by specific experiences in that situation but also, to some varying degree, by experiences in other situations that the individual perceives as familiar" (Rotter 1980: 2). Thus, large positive social changes can alter the environment and create trust. Through this he develops a hypothesis for generalized expectancy for trust or distrust and creates an additive test for interpersonal trust to be used in experiments (Rotter 1971: 445).

As expectancies for trust can develop from experiences, experiences can ultimately mean the difference between the level of trust in others and the different opportunities available to the individual. Hardin states that the capacity for trust is a "capacity that must largely be learned" (2002: 113). Judgments of trustworthiness are made "largely by generalization from past encounters with other people" (Hardin 2002: 113). Past experiences can differ by either being so positive that an individual can "optimistically take the risk of cooperating" with a stranger or by being so negative that an individual "pessimistically avoid[s] that risk" of cooperation (Hardin 2002: 113). The stranger "is no different in the two cases" but "prior experiences, unrelated to him or her, are the source of difference" (Hardin 2002: 113). Hardin acknowledges that if "past experiences too heavily represented good or poor grounds for trust, it may now take a long run of contrary expectations to correct initial expectations" (2002: 113). Reassessments based on evidence

of trustworthiness or untrustworthiness can change the initial skeptical judgment, but it is a process that takes time and willingness to be vulnerable: "Hence trust - the belief in another's trustworthiness - has to be learned, just as any other kind of knowledge has to be learned" (Hardin 2002: 114). As discussed, too much security in some areas can cause feelings of insecurity and suspicion about other people, environments or objects. But it cannot create the experiences of facing an untrustworthy individual needed to attain the belief that others cannot be trusted. As explained in the previous chapter, watching television is a form of leisure that is consumed for several hours a day, and it provides a type of continuous exposure to dangerous or risky behaviours that generates the belief that others are not trustworthy. Reinforced by visible security systems seen during daily activities, the televisual experience may create a generalized distrust in society, especially when danger can occur at anytime during daily activities. If the surveillance systems encountered are considered justified, they may also justify distrust. However, if there is too much security set up in one location and there is no experience of the violation of trust, then the surveillance might not cause any feelings of insecurity or distrust.

Experiences of trust that lead to a generalized trust in society can have beneficial outcomes as those who have initial judgments of high trust in others have different opportunities than do those with low trust in others. Distrusters face an unwillingness to be vulnerable that can substantially affect their ability to participate in meaningful interactions. Yamagishi has found that distrusters lack the social intelligence necessary "to differentiate [between] whom to trust and whom not to trust on the basis of very specific cues" (Cook, Hardin and Levi 2005: 23). In this way, "their lack of social intelligence

makes them more gullible when they do in fact engage in interactions", teaching them "to distrust others even more" because they fail rather than succeed in interactions (Yamagishi 2001: 122). Also, in "realizing their vulnerability, they avoid engaging in such interactions" that can lead to success or benefits thus losing potentially meaningful opportunities (Yamagishi 2001: 124). Thus having high trust gives us a "general optimism about the trustworthiness of others [that] enables us to enter mutually beneficial relations" (Hardin 2002: 114).

In his additive tests, Rotter found that "some people are more likely to be trusting than others" and from this developed tests with a differentiation between who he categorized as high trusters and low trusters. Like the difference in the levels of risk taking discussed in Yamagishi, Rotter's categories also differ in their level of cautiousness where "the high truster says: I will trust him or her until we have clear evidence that he or she cannot be trusted [and where the] low-truster in contrast says: I will not trust him or her until there is clear evidence that he or she can be trusted" (Cook, Hardin and Levi 2005: 23). High trusters are more likely to take risks whereas low trusters are not willing to make themselves vulnerable. In using these two categories of trusters, one of Rotter's additive tests discovered that high trusters "will permit a mistake or two and still trust providing the mistake is admitted and apology made" (Rotter 1971: 448). Rotter suggests, to a truthful degree, that this "point may be of significance for government and other institutions that have lost credibility of the public and hope to regain it" (1971: 448). Also, after reviewing several tests, Rotter is able to make some differences to gullibility between high trusters and low trusters. He states that "if trust is simply believing in communications in the

absence of clear or strong reasons for not believing and gullibility as believing when most people of the same social group would consider belief naïve and foolish, then trust can be independent of gullibility" (Rotter 1980: 2). To clarify, "to trust a stranger who has not lied to you before would not be gullibility; to believe a politician who has lied to you many times before is gullibility" (Rotter 1980: 4). In testing the differences of gullibility between high trusters and low trusters "no evidence was found that high trusters behaved in a way that can be called [...] more gullible than low trusters" (Rotter 1980: 4).

Using these tests can generate an understanding of why some still may trust the government and security systems when they fail. If and when a security system has failed, the government or security agencies have two options to restore trust. Firstly, if members of society have a high amount of trust, then a clear apology made by government or security agencies may minimize the effects of the mistake to a considerable degree, allowing for more security tactics to be adopted without much protest. Gullibility enables the second method, which would be to get rid of the failing security technology and replace it with a new one. Those that have a high level and a low level of trust would not be gullible because they have not seen this new system fail. The constant changes in security may also help lead to the expectation that security systems are always changing and create an easier adaptation to new security technology.

The Sense of Threat and Powerlessness

According to Mirowsky and Ross, who use the work of Rotter to discuss trust, distrust "makes sense where threats abound, particularly for those who feel powerless to

prevent harm or cope with the consequences of being victimized or exploited" (2006: 437). Thus, distrust can be amplified by feelings of "threat and powerlessness", which can be created by terrorism and security technology (Mirowsky and Ross 2006: 437). The all-encompassing threat of terrorism, with risk and weaponry taking "the familiar form of passenger jets, cars, computer code and even the daily mail", can create a threatening environment (Andrejevic 2007: 168). The vague descriptions of terrorist subjects and objects also play a role in constructing this environment because they transcend specific situations and enter everyday situations. Security technology causes a perpetual state of fear because it reminds us that we are vulnerable in numerous everyday situations and we constantly need protection from something or someone. Terrorism and security technology communicates that danger can occur at anytime; "it is almost impossible to predict or even imagine when and how attacks will occur" (Chan 2008: 228). This feeling of threat can create a sense of powerlessness, a "sense that one's own life is shaped by forces outside of one's control" (Mirowsky and Ross 2006: 438). It produces a loss of trust in others and culture of suspicion that can be "made up for by an increased reliance on vertical trust – the trust of political and security elites" (Chan 2008: 235). As a result, people may turn to security technologies, either in the hands of the government or in their own hands, as a form of control or protection from others.

The "sense of powerlessness that makes the effect of disorder or mistrust even worse" might be supplanted by a feeling of control gained by purchasing security technology (Mirowsky and Ross 2006: 438). This is because where powerlessness and a threatening environment amplifies the effect of threat on distrust, "a sense of control would

moderate it" (Mirowsky and Ross 2006: 438). If government attempts at providing security fails because the technology fails, feelings of powerlessness may be averted by giving citizens power in allowing them to use the technology as a form of protection. Though our "personal knowledge is [not] infallible", citizens may believe that the technology is being put to better use this way because "we tend to regard our own observations as more reliable, our interpretations as more sensitive, and our own judgements as more relative to our situation than those of other people" (Grovier 1998: 125). This may provide some relief regarding terrorism as threat "generates little mistrust among those who feel in control of their own lives, but a great deal among those who feel powerless" (Mirowsky and Ross 2006: 438). When citizens choose to use the technology for their own protection feelings of powerlessness can be decreased. The technology may bring about enough of a feeling of control that people can cope with personal security problems or feel that they have reduced their chance at victimization. However, security technology never seems to fully abolish fear because it can always act to remind us that danger lurks in the background of any situation. As such it may never be used to replace trust and only act to decrease trust because it instills feelings of suspicion. Perhaps only when threatening situations are not so frequently reported in the media and experiences of threat are lessened the consumption of security technology may subside.

Minorities and Trust Issues

Those groups who have been stereotyped and targeted by surveillance may already face issues with trust because their "individual disadvantage [of being marked by race] is

also associated with perceived powerlessness" (Mirowsky and Ross 2006: 439). People whose distrust is amplified by powerlessness and disadvantage may not have the same chances as those who have sources of power, such as those "with high incomes, educations, Whites and married persons"(Mirowsky and Ross 2006: 439-440). In turn, they may feel that they have no choice in some situations because the "outcomes of situations are determined by forces external" to them (Mirowsky and Ross 2006: 424). Race is permanently visible and as such it can be a marker of criminality and suspicion that can "set off more attention from agents of surveillance than others" (Glover 2008: 423, Chan 2008: 235). The mental stress caused by being frequently stopped by security forces can build and become damaging to one's sense of power; it can be a reminder to the citizen of colour of the "power relationship they are involved with the state" because it is the police who speak for the state and are constantly presuming guilt (Glover 2008: 244). Mental and physical well being can be sacrificed since "while racial profile processes interact with the body and the mind, the mental coercion that surrounds the encounters create unique alienating relations with the state that go beyond the physical" (Glover 2008: 246 - 247). In this way, these targeted groups face a form of alienation from those state departments that are supposed to protect them. It is a loss of innocence that reinforces unequal treatment by the state and communicates that people of colour do not have a chance to receive their desired outcomes - "the freedom from unwarranted state intervention" and the expectation to be protected by full economic and political rights as equal citizens (Glover 2008: 250, 245). 9/11 has acted to increase security checks on these groups and cause "'racially motivated' attacks, discrimination and harassment, threats, property damage and verbal

assaults in public against Arab, Muslim and Sikh Australians" by citizens encouraged to participate in the war on terror (Chan 2008: 234). Chan argues that "[t]he apparently pervasive and routine nature of such incidents suggests that the culture of suspicion has in fact developed into a culture of hatred" (2008: 233).

The consistency of threats, the lack of actual protection from police, and the feelings of powerlessness from being constantly stopped at security checks would certainly lower levels of trust in society by these groups. However, what Grover discovers is that tolerance seems to build from continual experiences as an interviewee in Grover's article states: "We just learn to accept it as part of our interaction with law enforcement" (Glover 2008: 253). Within minority groups and "communities of color, discussions about how to negotiate in a racial state become a part of community discourse. For young males of color in particular, a specific discourse about expectations from law enforcement is circulated as very purposeful communication for basic survival concerns" (Glover 2008: 253). This tolerance demonstrates that with enough experience an expectation begins to develop that can help a person get through the day without feeling like a targeted suspect. Some may begin to think that this is just the way things are handled, accept the procedures of security and move on. However, this tolerance does not build trust as it seems to be more the acceptance of system imperfections and distortions.

Security, Social Psychology and Trust

Overall, relying on security technology as a solution to safety issues may end up creating insecurity and further feelings of distrust. Making the fight against terror and risk

an individual problem can also spoil any chance at developing or maintaining trust because it takes away from social interactions that can build trust and actually provide feelings of security. Television programs and other media can be the sources that justify security technology, and security technology, in itself, can be a reminder that danger is found in all corners of everyday life. These both work to create a perpetual state of threat and feelings of powerlessness that can cause a generalized distrust between members of society. And where trust is lost in each other it is put into government, but this fails because its methods for safety do not always work. Trust also fails because the government puts responsibility back in the hands of individuals who relied to some degree and perhaps even trusted the government to begin with. In buying into security technology and participating in lateral surveillance to downplay the feelings of powerlessness we lose the ability to put trust in each other, which can actually be the source for safety. As Chan makes clear, "[i]f crime control is ultimately to engender social order and physical security, then a culture of suspicion is the anti-thesis of order and security because it undermines the ontological security of social interactions" (2008: 234). The only possible solution to creating trust in surveillance for security may be to "turn lateral surveillance on its head" (Chan 2008: 236). That is, "[b]y looking out for each other, instead of spying on each other, we may come close to the original idea of building strong and resilient communities" (Chan 2008: 236). In this way, the benefits and opportunities that come with trusting relationships may be attained as well.

Chapter 4

Resistance and Trust

As surveillance plays a significant role in contemporary society, so too is the recognition of its impacts, be it through movies, newspapers or other popular media. Although some surveillance devices have been made subtle and others rendered almost completely opaque, it does not mean that people are unaware of how some of their everyday lives are monitored (Lyon 2001: 127). While some may acquiesce to surveillance, others may feel the threat that surveillance generates and believe that they are vulnerable to privacy invasions (Lyon 2001: 127). To deal with problem large groups or organizations have been created to help resist surveillance and protect rights to privacy. Rights, however, do not always hold up in all surveillance situations, such as in trying to resist 'vancams' which photograph the license plate of speeders (Gilliom 2006: 111). Smaller movements by random, ordinary people are becoming more commonplace and performed on a daily basis. The seriousness of these movements can vary depending on how badly individuals want or need to resist surveillance, with some people resisting because the surveillance has been deemed sneaky or inappropriate and others resisting to be able move on with everyday life activities. Resistance, thus, may hold key issues of trust as it may be part of the reasons why people choose to resist, in that they decide the organization that is collecting the information is untrustworthy. It may also be an issue faced by those who are overwhelmed by surveillance because it demonstrates an absence of trust by the organization or institution conducting the surveillance. In some cases those surveilled are so underprivileged that they need to resist to survive, which raises questions

about how much trust they are offered and the extent to which a lack of trust can affect their lives. Importantly, as Gilliom points out, since surveillance is ubiquitous in modern society "resistance must be understood as acting within that context and not something that can prevent or undo it in any way" (2006: 114). Smaller movements made by individuals or small groups may be a new pattern of resistance that marks a "more definitive politics in our time" (Gilliom 2006: 122). To explain resistance, the work of Foucault, Lyon, Yar, Marx, Gilliom and Genosko will be discussed.

Power-Knowledge and Resistance

For Foucault, power, knowledge and resistance are linked together. He discusses how power and knowledge are connected as a type of "power-knowledge" (Foucault 1978: 98). They merge and are not external to each other for the reason that "different forms of discourse - self-examination, questionings, admissions, interpretations, interviews - [are] the vehicle of a kind of incessant back and forth movement of subjugation and schemas of knowledge" (Foucault 1978: 98). Power can demand knowledge and knowledge can attain control and power. Resistance is linked to power as "[w]here there is power, there is resistance" (Foucault 1978: 95). Points of resistance that "play the role of adversary, target, support, or handle in power relations [...] are present everywhere in the power network" (Foucault 1978: 95). This demonstrates that resistance should be expected everywhere that power is exercised, and because of this there is "no single great Refusal, no soul or revolt, source of all rebellions, or pure law of the revolutionary" (Foucault 1978: 95-96). Rather, power can be found everywhere and as a result there is a "plurality of resistances, each of

them a special case: resistances that are possible, necessary, improbable; others that are spontaneous, savage, solitary, concerted, rampant or violent; still others that are quick to compromise, interested or sacrificial" (Foucault 1978: 96). Resistance is an "irreducible opposite" of power that is "spread over time and space at varying densities, at times mobilizing groups or individuals in a definitive way, inflaming certain points of the body, certain moments in life, certain types of behaviour" (Foucault 1978: 96). In this way resistance is not aberrant. It is to be anticipated where there is power and can occur for different reasons to try to defy power. Surveillance can be understood as an attempt to exercise power by exerting control over secrecy and privacy. Eliminating secrets would allow knowledge to be accumulated about the private lives of individuals that could be used to control them. How this is resisted by large groups will be first discussed.

Resistance and Large Organizations

The majority of surveillance literature demonstrates that large organizational movements directed against surveillance are either failing or extremely limited. In his chapter "The politics of surveillance" Lyon (2001) makes clear points about why this may be occurring. Part of what hinders the success of resistance is the legal claim to rights. Privacy violations are popular claims as to why surveillance is harmful to the public; however the legal realm of data protection and privacy law has severe limitations as the "actual gains are far from earth shaking and social movements in this area are up against considerable odds" (Lyon 2001: 136). Lyon suggests that because features such as convenience, speed and security are involved with the use of technology, part of the

problem is that the "worrisome or unsocial" aspects appear merely as the price to pay for technological solutions or gains (2001: 136). Also, the effects of surveillance which work to disadvantage some groups over others "can be [merely] a side-effect of policies meant to achieve other ends" making it hard to fight using claims to rights because disadvantages to groups are not part of the overall goals (Lyon 2001: 136). This makes it easier for governments or corporations "that stand to gain from surveillance [to be in a] good position to make their case" thus allowing surveillance practices to be more acceptable (Lyon 2001: 136). In addition, companies can shape the way the public views the surveillance system or device (Lyon 2001: 139). Technology can be construed or constructed to be seen as "soft and malleable, it may be seen as something that can be shaped to appropriate ends or if necessary curbed" (Lyon 2001: 139). This flexible construction may reduce potential resistance because it can steer away from sharp criticism that definitive ends could create and change to allow for public approval (Lyon 2001: 139).

Other contributions to the limitations of resistance are the shortcomings of privacy rights as well as the lack of concern from the public. In the online sector privacy can be extremely limited for a number of reasons. First, cookies as well as other automated data collection programs are considered optional, but because of the browsing limitations when they are declined they are likely accepted. This restrains protection using privacy as a right because "regulations against selling personal information do not cover situations in which the user has 'consented' to share their information" (Yar 2006: 144). Second, since the Internet is comprised of various Websites that are unregulated, a problem of "legal pluralism" is created where "nothing prevents websites and information services located in

non-regulated or under-regulated territories from collecting and selling on such information" (Yar 2006: 144). This means that not only can users' information be collected without their knowledge, but that it can also be sold to the highest bidder, which in some cases can even include criminals (Yar 2006: 145). If these situations have not been publicized, they might not cause public concern as "culturally, in the U.S.A, privacy is not seen as an issue worth fighting for" (Lyon 2001: 138). This, Lyon points out, is in stark contrast to issues that are still being protested, such as the use of laboratory animals or biotechnology used to produce better pesticides and higher crop rates (Lyon 2001: 138). Not only may this be due, again, to a lack of useful rights and laws, but also because of acquiescence to surveillance procedures; there simply is not the same lightening rod effect with surveillance that helpless animals or the tampering of nature has on the majority of people (Lyon 2001: 139).

Personal Protection or Resistance?

Encryption is a technique or tool "associated with encoding or scrambling data in such ways as to render it incomprehensible to others not in possession of a 'key' that is needed to decipher the data into its legible form" (Yar 2006: 156). It is a form of resistance used by those who wish to avoid prying eyes and by those who wish to protect their personal information against potential hackers or criminals. It is used by "business and individual Internet users concerned about the possibility that their competitor or their or foreign governments may intercept sensitive communications" (Yar 2006: 149). However, because of the dilemma encryption can cause for criminal justice actors whose jobs include

detecting online criminals and reducing "the potential abuse of internet privacy by greater surveillance and monitoring of people's activities," the privacy and confidentiality of all online communications are at risk (Yar 2006: 140). These concerns of law enforcement agencies lead to attempts of the statutory regulation of encryption that were constantly debated by privacy campaigners (Yar 2006: 149). These debates continued over the past decade until the aftermath of 9/11 where "the tide finally turned in favour of law enforcement and against computer privacy activists" (Yar 2006: 150). Interestingly enough, the giving of encryption keys or the back doors of safety software to law enforcement agencies in reality does little to nothing to stop criminals or criminal organizations from creating better encryption with no keys or back doors (Yar 2006: 151). As a result, "the access acquired by law enforcement will prove ineffective in countering encryption used by professional criminals - its only use will be to enable surveillance of legitimate organizations and individuals" (Yar 2006: 151).

Since debates about the use of encryption technology continued for a period of a decade, the thoughts or attitudes of law enforcement and the state may have instilled cultural beliefs into the larger public about resistance to surveillance altogether. The sentences for encryption use that were proposed demonstrates the harsh punishments and labels put onto encryption users as, for example, a proposal launched in the UK had the trajectory in its "Electronics Communications Bill (1998) to allow law enforcement to demand keys from encryption users, with a failure to comply carrying a 'presumption of guilt' and resulting in a two-year custodial sentence" (Yar 2006: 150). Also, France, in "the mid-1990s, saw attempts to institute a public ban on so-called 'strong encryption', with the

state arguing that only those with something illegal to hide need have access to such security tools" (Yar, 2006: 149). In these cases, it can be understood that governments have attempted to exercise power to repress privacy and secrecy by labeling those who defy them as criminal. With such serious consequences and labels associated with a surveillance blocking tool some may have gotten mixed feelings about surveillance.

Marx, in his article "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance", speaks about the cultural beliefs that support surveillance (2003). Included are ideas such as "'It's for my own good' [and] 'I'm getting paid'"; he argues that "a lack of resistance to intrusive surveillance may mask as acceptance because of a fear of being sanctioned or losing one's job, position, or privilege" which relate to the consequences of being caught using encryption technology or other surveillance blocking tools (Marx 2003: 370). Marx also states that there may be a "lack of awareness of the extent and nature of surveillance, or of the potential for abuse and misuse of personal information [which] may also support acquiescence" (2003: 371). At the same time, the discourse on encryption and other methods of avoiding surveillance demonstrates how governments were trying to gain control over people's beliefs about surveillance. Power was exercised in an attempt to repress secrets and hiding information. This was met by the endeavours of privacy activists to protect citizens from privacy violations. Although these efforts failed, it does not mean that resistance against surveillance has stopped. Rather, it has taken on a new form of small group or individual resistance. A question of trust that can be posed from this discussion is whether society views those who try to hide information as untrustworthy?

Small Group Resistance

The failures or limitations of large organizations to resist surveillance demonstrate that resistance may be more productive when it is performed by smaller groups of people or individuals. Indeed, small scale attempts are practiced on an everyday basis by ordinary people who achieve "short term gains that are important to daily life" (Gilliom 2006: 113). These movements may be more successful and easier to conduct because of the way surveillance is set up. As Genosko makes clear in his chapter "(Im)Possible Exchanges", the possibility of why smaller resistance movements may be more frequent and productive is because when "certain technologies are defined along Giddens's lines through the concept of distanciated observation, response becomes extremely difficult and, perhaps most importantly, counter-surveillance is limited to a small group or individual affair rather than a widespread practice" (1996: 33). Gilliom makes a related point, in that with no "grand and visible displays of power over groups of people, it should hardly surprise us that forms of opposition and resistance are equally discreet *and* discrete" (2006: 121). Surveillance technologies or control systems "are not usually as effective and efficient as their advocates claim and they often have a variety of unintended consequences" (Marx 2003: 371). Some of these consequences can provide a breaking point through which people begin to feel the need to resist. But more importantly, the unperfected surveillance gives an open space in forms of "inherent contradictions, ambiguities, gaps, blind spots and limitations" through which "surveillance targets have a space to maneuver and use counter-technologies" (Marx 2003: 372).

As Marx claims, individuals are "often something more than a passive and

compliant reed buffeted about by the imposing winds of the more powerful, or dependent only on protest organizations for ideas about resistance. Humans are wonderfully inventive at finding ways to beat control systems and avoid observation" (2003: 372). With that said, Marx discusses eleven generic techniques of surveillance neutralization that are used by the strong, as well as by the weak (2003: 372). These techniques can indirectly neutralize surveillance - such as discovery moves in which a person attempts to find if surveillance is in operation and to locate it, avoidance moves in which a person avoids the surveillance upon discovery, and blocking moves in which a person covers certain items that can be identified. These techniques can also be drastic movements that directly neutralize surveillance - such as using breaking moves in which a person tampers with or destroys a surveillance mechanism, refusal moves in which a person outrightly refuses to be surveilled, or masking moves in which a person replaces blocked information with misleading information (Marx 2003). Each can be performed by amateurs or experts, legitimate persons or illegitimate persons. But an important point is that the cultural beliefs for why surveillance is resisted are based on issues of distrust, such as not trusting the company to keep information confidential, thinking that the collection process is sneaky, and believing that surveillance is distrusting the legitimate person (Marx 2003: 373). These reasons for resistance differ based on the context of the situation, which also demonstrates that the level of trust differs based on the context as well. Levels of resistance also differ with levels of power as those who are under more control may find it harder to resist and may resist for different reasons than those who are under less. This will become clearer in the discussion of Gilliom's work on welfare users.

Resistance occurs mostly "when individuals feel that the surveillance is wrong, or feel that they are unfairly disadvantaged by it" (Marx 2003: 372). It may also occur as a challenge performed out of pleasure or "for reasons of self interest" (Marx 2003: 372). Marx notes that "people will break rules if they regard an organization or its surveillance procedures as unacceptable or illegitimate, untrustworthy, or invalid, demeaning, unnecessary, or irrelevant" (2003: 373). These reasons for resisting are important because they show that privacy, which is used as the "vast bulk of responses to surveillance", is not the defining factor for resistance (Lyon 2001: 128). Resisting surveillance is mostly made up of "spontaneous mobilizations that pose a range of challenges from the non-serious to serious" (Genosko 1996: 33). They include personal, private beliefs that cannot always be fought for by legal means or under the right of privacy. This means that each personal situation of surveillance differs by intensity, consistency, and context. Thus, the subjects of surveillance and the reasons why they are surveilled must be looked at to fully understand the reasons for resistance and whether it can be viewed as legitimate or illegitimate.

In "Struggling with Surveillance: Resistance, Consciousness and Identity", Gilliom focuses on the subjects of surveillance, and their perspectives and understandings of being watched. He explains that young mothers and their families are the primary users of a welfare system in Ohio (Gilliom 2006: 115). They are thus monitored by a computer system known as the Client Registry Information System - Enhanced (CRIS-E) which "manages all case information about welfare clients in the state, storing and handling data pertaining to identity, paternity, health concerns, employment and educational history, financial need, and any other of the myriad points of information collected by the welfare

system" (Gilliom 2006: 115). Since this system is combined with the "widely distributed posters and ads about the evils and dangers of welfare fraud", the constant questioning from caseworkers, as well as the constant threat of potential blackmail from neighbours, former spouses and virtually anyone who "can choose to report them, invoke dormant rules or instigate investigation", the impact and experience of surveillance of these women make them "valuable experts on the nature and politics of surveillance" (Gilliom 2006: 115-116). Under all this pressure, these women are compelled to resist the confusing and restrictive rules of the welfare system to secure extra money to make up for the inadequate amount given to support families. From several interviews with these women, Gilliom discovered that adding to the stress that could be caused by errors from caseworkers, most women expressed fear that they would be caught; "It's scary and if you are not worried about not being able to feed your children or have a home to sleep in you are worried about whether you are going to go to prison for welfare fraud" (2006: 117). Also discovered through Gilliom's analysis is that the women did not make mention of the right to privacy (Gilliom 2006: 118). Rather, the explanations for resistance made by them were with reference to needs and to provide for their families what the state did not; "a pattern of resistance that has clear results: desperately needed material benefits; the maintenance of a zone of autonomy in the face of dependency of life on welfare; the sustenance of a shared identity of mothering; and the undermining of the surveillance mission itself" (Gilliom 2006: 118). This demonstrates that the "frontline battle against [this] system of surveillance appears to be rooted in the everyday struggle to get by" unlike other cases where resistance may be simply carried out to maintain privacy (Gilliom 2006: 119). This analysis speaks to the

importance of context when attempting to understand trust, as with the addition of surveillance demonstrates a decrease in the amount of trust. Does this portrayal of welfare users show that they are untrustworthy by the institution? Also, does their situation show that they are deserving of this amount of suspicion (Gilliom 2006: 124)?

Resistance and Trust

Conceptualizing trust in this context is important because it can be seen as a driving force for resistance. As Gilliom makes clear "it is the case that surveillance programs are *different* for those who are wanting or needing to deviate from the norms and those who are not" (Gilliom 2006: 125). If this is the case then trust also differs depending on the context of the surveillance situation. Where power is a factor that can enforce surveillance, levels of trust or distrust may also vary according to the levels of power. As seen in the case of encryption those who resist may be viewed by the state, or even society, as untrustworthy or criminal; however those who resist may do so because they view the state, institution or organization as untrustworthy. If resistance is undertaken on a daily basis by most people, questions can be raised about whether members of society view the state or each other as untrustworthy. Are resistors really seen as untrustworthy? In addition, those who are under extreme situations of surveillance, such as the women and their families on welfare, must resist to support their families. The overwhelming surveillance they face may demonstrate an absence of trust and may change how they are viewed by society. Are those that are more closely watched seen as less trustworthy? Is this only viewed by those who are watching them or society as a whole as well? The definition of trust that will help to answer

some of these questions will be derived from philosophy.

Philosophy and Trust

Some philosophers, such as Glaucon, Machiavelli, Hobbes, Locke and Kant, have attempted to explain their perspectives on trust and justify when it is appropriate to consider. However, trust in philosophy is an elusive concept as philosophers "often simply ignore it or presuppose it, and when they do consider it, they often struggle to explain it or confuse it with other things" (Bailey 2002: 1). To develop an understanding of philosophical trust the perspectives of these philosophers will be explained as well as more modern philosophical literature from authors Grovier and O'Neill who include a social insight to help explain trust. The definition will be taken from Grovier in which trust "is in essence an attitude of positive expectation about other people, a sense that they are basically well intentioned and unlikely to harm us. To trust people is to expect that they will act well, that they will take our interests into account and not harm us" (1998: 6). Taken together, these theories can help explain how surveillance may seem to work as a replacement for trust when there is distrust and how it works to cause distrust or resistance. The philosophical understanding of trust largely takes the context into consideration, which makes it significant when relating to resistance.

The conceptualization of trust by early philosophers was developed on the basis of how they perceived the state during the times of their writing. Glaucon, Plato's older brother, Machiavelli and Hobbes all saw worlds in which people were self-interested. From a story he once heard about a man who when gone undetected embarked on

mischievous behaviour, Glaucon argued "that only the fear of detection and punishment prevents a human being from breaking the law and doing evil for the sake of his own self-interest" (Bailey 2002: 1). To know when it is right to trust someone he suggested that "we should trust others only if we are confident that they fear detection and punishment sufficiently to dissuade them from harming or stealing from us" (Bailey 2002: 1). The surveillance society, then, should be able to stop all from committing criminal acts; however this is not the case. Rather, people will continue to steal and vandalize in front of surveillance cameras. Following Glaucan, Machiavelli states that in case the fear of punishment and detection are not enough, and also so as not to be vulnerable to others, one must "be prepared to be cruel, murderous, dishonourable, deceptive, and miserly whenever necessary to maintain their power" (Bailey 2002: 1). This means that those who must trust are in a vulnerable state and must be prepared to strike in the chance that those who are trusted choose to attack. Thus the "distrust and attacks will spiral, ending only with the victory of the most brutal and cunning" (Bailey 2002: 1). In an attempt to prevent an imminent war from this problem of trust, Hobbes believed in the idea of a mutual truce or agreement as a solution. He, unlike the others, recognized "that we might wish to agree to a truce amongst ourselves, an agreement to restrain the pursuit of self-interest when necessary to avoid war" (Bailey 2002: 2). The problem with the idea of the truce, he suggests, is that it may be irrational as not everyone may follow it after it is made. Partly, this is due to the advantages that could be taken up by an individual or group in breaking the agreement, and also because one may "reason badly, fail to consider the future, or are carried away by other feelings" such as obsessions or anxieties (Bailey 2002: 2). Thus a

truce would likely not work because of "the prevalence of irrationality among human beings, the uncertainty of knowing who might act irrationally, and when, and the huge risks involved in keeping to the agreement" (Bailey 2002: 2). Ultimately, "Hobbes concludes that even those rational enough to wish that the agreement be kept would be foolish to keep it" (Bailey 2002: 2).

These theories show great distrust in society; a place where only fear and threats may be the only possible ways to create any sort of trust in others. If society did work in this way we would all be completely exhausted from trying to resist all potential attackers every day. Fortunately, Hume was a philosopher who reasoned that not everyone at every time was self-interested to this extent. He recognized "that human beings naturally care for their loved ones and sympathise with others' feelings, including those of complete strangers" (Bailey 2002: 3). Though he admits sympathy and love may be not enough reason to trust because there is always the chance that bonds between brothers can be ruined from self-interest, Hume does state that a way around this may be through putting faith in other areas "such as education and civilization to improve and spread out sympathy for others, and thus reduce the likelihood of distrust and war" (Bailey 2002: 3). A shared sense of morality may help get rid of selfish desires as Locke and Kant argued that morality "might be cultivated to overcome the partiality of self-interest" (Bailey 2002:3). At the end of his discussion, Bailey suggests that what is not included in these arguments is a sense of genuine trust (Bailey 2002: 4). He recognizes that in order for someone to even achieve immoral or unjust ends; there must be the "possibility of relying on each other to behave and respond in predictable, manageable ways [which] is particularly valuable for human

beings" (Bailey 2002: 4). In this case, people must be "taking responsibility for how their behaviour will influence [others'] decisions about how to act in a particular regard" (Bailey 2002: 4). Importantly, he argues that "one cannot genuinely trust others if one resorts only to reliance on detection, punishment, love, sympathy, or a sense of morality, [but that] one can certainly make some use of such resorts without necessarily failing to trust" (Bailey 2002: 4).

Society may not be as full of selfish individuals as some philosophers have insisted, but in the end they do bring up important points about distrust and recourse used to help in situations defined by lack of trust. It is not possible to completely trust or distrust because they are both "susceptible to degrees: [where] we may trust or distrust someone slightly, moderately, or completely" and also because "[b]oth attitudes are often relative to contexts: [where] we might, without hesitation, trust a person to deliver a parcel and yet feel ambivalent about trusting him to repair a computer" (Grovier 1998: 121). This means that distrust can be expected in some situations, but the more that "trust is deep and complete makes a harmful act more shocking" (Grovier 1998: 142). Relying on detection, punishment or other means to be able to trust others may be a way that society combats feelings of distrust. In this case, the use of surveillance would suggest that society distrusts government and vice-versa because surveillance is found in both realms. The surveillance in government institutions could create the potential for society to trust the government because society can see that the government is doing its job properly. It may be used to thwart feelings of distrust. However, these techniques may also be seen as attempts to exercise power and cause resistance even by government workers. The next section will

discuss some further techniques to combat feelings of untrustworthiness.

Combating Distrust

To solve a problem of distrust there are a few methods that can be used. A person may "try to manage some aspects of the relationship by appealing to rules" (Grovier 1998: 155). However, where "we are inclined to appeal to rules" due to a lack of trust, "the less useful those rules are likely to be" (Grovier 1998: 155). This is because the "negotiating, agreeing on and complying with rules *presupposes* trust" (Grovier 1998: 155). Situations may be encountered that the rules do not cover and "where there is trust we assume that they [those trusted] will be flexible and reasonable in working to solve unanticipated problems" (Grovier 1998: 158). As such, "[f]or rules to work, we need confidence in other's good judgment and goodwill", in distrusting "we feel the need for some *guarantee* that the other will do *what is required* when a problem arises. And no such guarantee can be contained in the rules themselves" (Grovier 1998: 158). In this case, appealing to rules cannot be used to reduce distrust and leaves the issue of distrust unresolved. Using contracts is another method that can potentially lower feelings of distrust. Grovier notes that "[t]hough helpful on occasion, they do not eliminate the need for trust"; contracts are "at best a partial strategy for managing distrust" (1998: 158). They can even hinder trust as the "very suggestion that arrangements should be formalized in writing can destroy trust" (Grovier 2007: 53). Again, the issue of trust is not resolved leaving either party potentially unsatisfied. There is also the idea of using the law to solve problems of distrust. However, issues of trust are left unsettled as "laws do not by themselves change attitudes" (Grovier

1998:162). Law's use "may be a factor in monitoring restraint and safety, and it may prevent people from physically terrorizing each other [but] legal proceedings and injunctions in themselves do little to nothing to address problems of distrust" (Grovier 1998: 163).

Grovier explains the idea of controlling and the exercise of power as another way to reduce distrust that fails. Controlling others may be a response to distrust which can be an especially "tempting response for parents or others who are in a position to exercise power" (Grovier 1998: 158-159). In attempting to exercise power, especially in situations of unequal power distributions "[e]fforts to control imply a lack of trust or confidence" that "breeds [feelings of] untrustworthiness and more distrust, and eventually control leads to resentment and rebellion" (Grovier 1998: 159). This is especially the case when those upon whom power is exercised have "any aspiration for autonomy" (Grovier 1998: 159). There is no opportunity for those controlled to truly be themselves or show that they are trustworthy, and it is likely that those, such as children, who "have been too strictly controlled [...] strike out in rebellion the moment they can gain their freedom" (Grovier 1998: 159). Where power is at an equal level between individuals or groups, "control is even less promising as a response to situations of distrust" because the "potential for exercising control is quite limited" (Grovier 1998: 159). The attempts at controlling in these cases can be ineffective and counter-productive as it may only inspire resistance (Grovier 1998: 160). Surveillance, Grovier explains, is "an attempt to extend control (or the potential for it) to occasions when one is not present" (1998:159). Using surveillance can actually solve distrust, but only very rarely and in situations where it can be used to

prove that someone is trustworthy (Grovier 1998: 159). Using excessive amounts surveillance can entail "serious invasions of privacy and high costs to the relationship involved if and when it is discovered" (Grovier 2007: 53). Controlling or exercising power over others in all cases "undermines the autonomy of others" and alienates them from the controllers (Grovier 1998: 161). It is ultimately seen as an "expression of distrust" (Grovier 1998: 161). Therefore, all who attempt to exercise power have the potential to be seen as distrustful, and this becomes even worse for those who have equal levels of power as their attempt to control can appear as "manipulative and domineering" (Grovier 1998: 160). As a result, where there are opportunities people will resist.

In each case, one person or group may be understood as attempting to exercise power over another by using rules, contracts, the law, control or surveillance. Whereas trusting can make some feel empowered and worthy, these methods fail because they demonstrate an absence of trust and hurt the development of autonomy of the other person or group. As a result those controlled may understand that they are perceived as untrustworthy and resist or rebel. Part of the danger in causing distrust is that regaining trust may not be so easily done as "even evidence of positive behaviour and intentions [...] is likely to be seen with suspicion, to be interpreted as misleading and, when properly understood, as negative after all" (Grovier 2007: 52). Also, the costs of distrust may include a lack of openness, strong pressures "to pretend an acceptance of others even when we do not feel it" and a sense of unease about those we distrust (Grovier 2007: 53). Though "when we distrust someone when we doubt that he is what he purports to be, social convention almost requires that we disguise our own attitude, hide our doubts and pretend

all is well", forms of surveillance that cause feelings of obvious distrust can have more serious reactions (Grovier 1998: 145). "In making explicit the sense that the affected people are regarded as potentially untrustworthy, these policies tend to evoke feelings of alienation, hurt, and/or disloyalty resulting in unwillingness to go the extra mile, working to rule, lack of commitment to the organization, people, and tasks involved, or even cheating and dishonesty" (Grovier 2007: 53). Resistance will follow because of the distrust and the undermining of autonomy created by surveillance and control.

Welfare Users and Distrust

In the case of welfare users, there is an extreme power differential between them and the government. They may not display or express signs of distrust, but their position and situation make them easy targets for surveillance. In exercising power through surveillance and the CRIS-E system, the attempt at control demonstrates signs of distrust. The context of their situation, where they live in "something closer to the original idea of the Panopticon than others who must face not so much a singular and powerful omnipresence, but rather numerous checkpoints", makes it evident that there is almost a complete absence of trust (Gilliom 2006: 124). This harms welfare users as they complain "about degradation and humiliation" and it undermines their autonomy as capable mothers who provide for their families (Gilliom 2006: 123). Their ability to resist and make extra money shows an open gap in the routine of surveillance. However, the control that they are under does not allow them very much room for resistance. Their resistance does not

demonstrate a problem of distrust, but rather a problem of survival and getting by; they must resist to survive. They understand the distrust that they must fight by providing proof that they are not receiving any extra income. The method of surveillance is not providing any kind of trust and can act to damage it by causing fear and unease in those being watched. The extreme amount of control creates a different force for resistance than distrust, but shows how surveillance has severe implications to those being watched.

How Distrust Begets Resistance and More Distrust

O'Neill discusses the problem of distrust that is faced by the government from society in the UK. Her analysis demonstrates just how well surveillance works at hampering and dampening trust. A problem of distrust has been raised because "a look at past news reports show[s] that there has always been some failure and some abuse of trust" (O'Neill 2002: 44). The supposed remedy to this suspicion "lies in preventions and sanctions" or fear of punishment where "[g]overnment, institutions and professionals should be made more accountable" (O'Neill 2002: 45). For those working in the public sector, this call for more accountability "takes the form of detailed control" through strict legislation and regulation (O'Neill 2002: 46). What is required is "detailed conformity to procedures and protocols, detailed record keeping and provision of information in specified formats and success in reaching targets" (O'Neill 2002: 46). These solutions to distrust resemble rules, contracts and surveillance discussed by Grovier. The standards that are produced to ensure that public needs are being met can resemble a type of power that is

exercised by society. It is a demand for more transparency which represses and destroys secrecy and any plot that the government may have to exploit taxpayers, "but it may not limit the deception and the deliberate information that undermine relations of trust" (O'Neill 2002: 70). This is because "[t]ransparency can encourage people to be less honest, so increasing deception and reducing reasons for trust: those who know that *everything* they say or write is to be made public may massage the truth [...] Demands for universal transparency are likely to encourage the evasions, hypocrisies and half-truths that we usually refer to as 'political correctness', but which might more forthrightly be called either 'self-censorship' or 'deception'" (O'Neill 2002: 73). An increase in transparency can damage trust because it creates a "flood of unsorted information and misinformation" that adds to "uncertainty rather than to trust" (O'Neill 72-73). O'Neill demonstrates that even those in government can use resistance techniques to hide the full truth. This leads society to further distrust the government because they cannot sort the information into truth, lies or half-truths. Also, the technology takes away from any sort of active inquiry, which is done "over time by talking, asking questions, [and] by listening", that can be used to help build trust (O'Neill 2002: 76). Both government institutions and society are at a loss in this situation as more distrust is created from various forms of resistance and surveillance. Surveillance does not seem to help the situation, and instead can be conceived as fuel for the fire.

Resistance, Philosophy and Trust

Surveillance can be understood as a form of control that makes some people feel

threatened and others untrustworthy. Surveillance can be used to try and combat distrust, but it is almost always unsuccessful. In very rare cases it can be used to prove trustworthiness, but this is in the form of a revindication. It actually helps to put resistance in motion because of these feelings of distrust it creates. However, as seen in O'Neill's analysis, surveillance and distrust begets resistance and more distrust, which creates a push for more control and more surveillance. Tight and unreasonable controls such as in the case of welfare users, can stop resistance that is performed for reasons of distrust and create resistance for purposes of survival. In any case, surveillance does not provide much or any room for trust, but can damage it and feed the fire for resistance.

Conclusion

Surveillance is present in all aspects of daily life. It perfuses all environments - offline, online, work, home and play - and is necessary to establish the identity of strangers. Trust is necessary as well for people to enter into various social situations feeling secure and confident (Grovier 1998: 86). Both aspects are important for a thriving society; however, where surveillance can hold society together, it can also be what hinders the development of relationships and erodes the levels of trust in society.

Each key theme in the surveillance literature was reviewed with certain aspects discussed in detail. Questions of trust were posed on the basis of each discussion. Trust was defined or conceptualized according to the corresponding discipline that cohered with the surveillance theme and contributed to the analysis. The definition was used to try and explain whether the situation of surveillance was working to negotiate, manipulate, replace, build or damage trust. The definitions could not provide full explanations of all of the aspects of surveillance in each theory, but were helpful in explaining why surveillance modified trust. The research has provided a discourse analysis where disparate literatures - those on surveillance and trust - were discussed and productively tied together.

Examining surveillance and trust has made it clearer that trust is very rarely built or fostered through any type of surveillance technology or technique. Each theme examined in the four areas of social surveillance theories provided evidence of the dangers and damages surveillance has on various aspects of everyday life. When questions of trust were posed and analyzed through definitions of trust borrowed from different disciplines some of the reasons why surveillance does not or cannot foster trust were discovered.

In summary, my findings may be presented in two categories that add to the re existing schema presented in the introduction.

	Linkages and Contexts	**Issues and Outcomes**
1.	Automated personal information gathering online and abstractions of data mining; Illusion of consent	Manipulation of trust by sellers in a climate of generalized distrust of e-commerce; Dehumanizing consumers by technical distancing; Coerced trust and manufactured consent
2.	Disciplinary media spectacle as a silencing device; Panoptic/ synoptic parallels	Trust as a diminished social and public benefit; False idols of interpersonal intimacy (for example, television personalities); Online communities without obligations and tools to build collective values
3.	Technologization of security substitutes for policy development; Surveillance as security constructs insecurity, anxiety, fear, suspicion and racial hatred	Profiling precludes trust; Security as a consumer good is self cancelling, de-socializing and isolating; Only large scale social change could restore trust; Restoration of trust through transparency and public admissions are insufficient; (in)Security conditions citizens to accept new security technologies
4.	Trust is context sensitive; Microresistance exists at every point of microphysics of power; Limits of legal recourse; Curtailed encryption	Resistance exploits cracks in imperfect surveillance; Distrust is the engine driving creative resistance; Spiral of distrust is interrupted by survival; Very rarely surveillance "proves" trust as revindication

The main purpose of the Panopticon is to discipline bodies through a method of surveillance that ensured an automatic functioning of power. Today, the electronic Panopticon collects information, analyzes it and makes predictions. It ultimately collects more knowledge that is used to gain power. Trust was apparent in the relationships formed

after information was divulged through the illusion of voluntariness. In order to continue the flow of information that is significant to most companies, relations would need to be maintained with customers, which suggested a development of trust. The business discipline provided some online techniques that could be used to gain and maintain trust between consumers and businesses. Ultimately, it was understood that in most cases businesses were more interested in collecting information and managing customers than in actually maintaining trust out of concern for the consumer. This demonstrated a manipulation of trust.

In analyzing the synopticon, it was found that the many watching the few did not act to create any forms of trust between individuals. It was hypothesized that trust could be developed from the interactions that could start up from interests in familiar television shows or developed in online communities made up of various forums where people could post personal information to strangers. Sociology analyzed trust as a function through which many benefits could be gained, so the analysis of trust focused on whether the elements of the synopticon could build trust that support its various functions. Using the technology to try and build trust was found to be unsuccessful. Watching television actually acted to decrease time spent in activities that could support functions of trust. The familiarity of television programs acted as grounds for communication, but these interactions were found to function weakly and hamper the potential for sustaining and creating meaningful relationships. Also, television could reinforce that certain members of society or certain areas of society are not to be trusted. Online communities were found to fail at developing trust because they only develop an artificial sense of community. The

disconnected and disembodied interactions between individuals are not backed by trust. Online communities also failed to support functions of trust because they could not build values as traditional communities could. This is because they are linked to bureaucracy and law, which take over in cases where values are lacking. Overall, elements found in the synopticon could not produce the basis to facilitate functions of trust.

Security, in itself, creates feelings of distrust and insecurity. Though security technology can be found in almost every building, 9/11 acted to enhance and massify security surveillance and techniques. Defense and protection from risks since 9/11 has been made into more of an individual problem and certain groups have been screened and targeted more by security. Social psychology provided an understanding of the importance of experience, and the effects of threat and powerlessness that influence decisions to trust. Consistent reports of terrorism on television create an environment of perpetual fear, with terror occurring in seemingly normal situations. It can justify surveillance technology which, in turn, also reminds society that danger lurks around every corner. Surveillance technologies may be consumed to gain a sense of power, albeit a false one, that can protect against the everyday threat of terrorism. Those profiled groups who are targeted by surveillance face the distrust of government in the guise of the police officers that constantly stop them for unjustified reasons. It undermines them as citizens who deserve equal rights. Taken together, this security undermines the development of trust and even the social interactions that can be used to build trust and an actual sense of security.

Foucault's microphysics of power entails microresistances. Several reasons have been suggested as to why some people resist surveillance or acquiesce to its procedures.

Surveillance suggests an absence of trust, and whether this is backed by actual feelings of distrust or not, it will be resisted. Philosophy has worked well to explain the consequences of using surveillance as a technique to combat feelings of distrust. It can create feelings of distrust or undermine autonomy which mobilizes acts against it. Resistance to surveillance is acted out both by members of society who are watched by the government and acted out by government employees who are monitored by society. Resistance makes it even more difficult to trust, which suggests the almost complete failure of surveillance to produce or support any form of trust. At best and rarely, surveillance can prove trust exists after the fact of distrust. Importantly, philosophy taught that exiting the spiral of distrust for the sake of survival is a tactic that does not restore trust, but trumps distrust. It is evidence of state violence by means of surveillance.

The intention of this thesis was to understand whether surveillance is acting to negotiate, manipulate, replace, build or damage trust. This research shows that surveillance works to damage or manipulate any type of trust in society. It cannot work to build, foster or maintain trust. Surveillance is manipulating trust in some cases, acting to damage it and preventing its onset in others. Overall, the use of surveillance does not convey trust or supply space for trust to build. Trust is not developed through watching television or divulging personal information. It is not fostered by security surveillance that is supposed to make people feel safe. It is not a large deal to businesses who manipulate trust to gather more information from online users. And finally trust is not created by surveillance as surveillance seems to motivate distrust that mobilizes resistance and reduces chances of creating autonomy.

This research has also made clear how truly important trust is and why it is the glue of society (Grovier 1998: 6). Destroying or damaging trust can have results that are quite severe and detrimental. This makes it vital to continue research on trust. Surveillance does not seem to be a source for any type of trust; however it does not completely damage or destroy trust as we still continue to put trust in systems, people and objects. Further research could be done to try and discover how trust is maintained in small acts and how it is built against most odds. Finding sources of trust and supporting them could help increase trust or at least prevent it from further decreases.

Our world may not be as dystopian as Orwell imagined, but surveillance does seem to work in some of the ways that he describes. It seems to blur the boundaries between the watched and the watchers. It certainly can act to make some people fear their own actions in front of cameras and other people, while at the same time it can make us cautious of seemingly normal behaviours of others. It changes the levels of trust in society, but this depends on various aspects, such as context, past experiences, and beliefs. In the end, surveillance does not completely destroy trust. Trust still exists in society, but it is not supplied or created by surveillance.

Bibliography

Aas, Katja, Gundhus, Helene and Lomell, Heidi, ed. 2009. *Technologies of InSecurity: the surveillance of everyday life*. New York: Routledge-Cavendish.

Andrejevic, Mark. 2007. *iSpy: Surveillance and Power in the Interactive Era*. Kansas: University Press of Kansas.

Bailey, Tom. 2002. "On trust and philosophy." *Philosophy and Ethics*. British Broadcasting Company. Retrieved January 5, 2010. (http://www.open2.net/historyandthearts/philosophy_ethics/trust_and_philosophy.html)

Better Business Bureau. 2010. "Vision, Mission and Values." Canadian BBB. Retrieved January 12, 2010 (http://www.bbb.org/canada/BBB-Mission/)

Bigo, Didier. 2006. "Security, exception, ban and surveillance" Pp. 46-68 in *Theorizing Surveillance: The panopticon and beyond*, edited by D. Lyon. Oregon: Willan Publishing.

Cook, Karen, Hardin, Russell and Levi, Margaret. 2005. *Cooperation Without Trust?* New York: Russell Sage Foundation.

Chan, Janet. 2008. "The Lateral Surveillance and a Culture of Suspicion" Pp. 223-239 in *Surveillance and Governance: Crime Control and Beyond*, edited by Mathieu Deflem. Bingely: Emerald Group Publishing Limited.

Doyle, Aaron. 2003. *Arresting Images: Crime and Policing in Front of the Television Camera*. Toronto: University of Toronto Press.

Elmer, Greg. 2004. *Profiling Machines: Mapping the Personal Information Economy*. Cambridge: The MIT Press.

Foucault, Michel. 1977. *Discipline and Punish: The birth of the prison*. New York: Pantheon Books.

Foucault, Michel. 1978. *The History of Sexuality Volume 1: An Introduction*. New York: Pantheon Books.

Frankel, Tamar. 2006. *Trust and Honesty: America's business culture at a crossroad*. New York: Oxford University Press.

Gandy, Oscar. 1993. *The Panoptic Sort: A Political Economy of Personal Information*. Colorado: Westview Press.

Gandy, Oscar. 2006. "Data Mining, Surveillance, and Discrimination in the Post 9/11

Environment" Pp. 363-384 in *The New Politics of Surveillance and Visibility*, edited by Kevin Haggerty, and Richard Ericson. Toronto: University of Toronto Press.

Genosko, Gary. 2005. "(Im)possible Exchanges: The Arts of Counter-Surveillance" Pp. 31-50 in *Canadian Cultural Poesis: Essays on Canadian Culture*, eds. Garry Sherbert, Annie Gérin, Sheila Petty, Waterloo: Wilfrid Laurier University Press.

Giddens, Anthony. 1991. *The Consequences of Modernity*. California: Stanford University Press.

Gilliom, John. 2005. "Struggling with Surveillance: Resistance, Consciousness, and Identity" Pp. 111-129 in *The New Politics of Surveillance and Visibility*, edited by Haggerty, Kevin D., and Ericson, Richard V. Toronto: University of Toronto Press.

Glover, Karen. 2008. " Citizenship, Hyper-Surveillance and Double-Consciousness: Racial Profiling as Panoptic Governance" Pp. 241-256 in *Surveillance and Governance: Crime Control and Beyond,* edited by Mathieu Deflem. Bingely: Emerald Group Publishing Limited.

Goold, Benjamin. 2009. "Technologies of surveillance and the erosion of institutional trust" Pp. 207-218 in *Technologies of InSecurity: the surveillance of everyday life*, edited by Katja Aas, Helene Gundhus and Heidi Lomell. New York: Routledge-Cavendish.

Grovier, Trudy. 1998. *Dilemmas of Trust*. London: McGill-Queen's University Press.

Grovier, Trudy. 2007. "Distrust as a Practical Problem." *Journal of Social Philosophy*. 23(1): 52-63.

Haggerty, Kevin and Ericson, Richard, ed. 2006. *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press.

Hardin, Russell. 2002. *Trust and Trustworthiness*. New York: Russell Sage Foundation.

Henslin, James, Glenday, Dan, Duffy, Ann, Pupo, Norene. 2004. *Sociology, A Down-to-Earth Approach: Third Canadian Edition*. Toronto: Pearson Education Canada.

Innes, Martin. 1999. "The Media as an Investigative Resource in Murder Enquiries. *British Journal of Criminology*. 39 (2): 269 - 286.

Kumpost, Marek and Matyas, Vashek. 2009. "User Profiling and Re-identification: Case of University Wide Network Analysis" Pp. 1-10 in *Trust, Privacy and Security in digital business: 6th international conference*, edited by Simone Fischer-Hubner, Costas Lambrinoudakis, and Gunther Pernul. New York: Springer.

Luhmann, Niklas. 1979. *Trust and Power*. New York: John Wiley and Sons.

Lyon, David. 1994. *The Electronic Eye: The rise of surveillance society*. Cambridge: Polity Press.

Lyon, David. 2001. *Surveillance Society: Monitoring everyday life*. Philadelphia: Open University Press.

Lyon, David. 2003. *Surveillance After September 11*. Cambridge: Polity Press.

Lyon, David. 2006a. " 9/11, Synopticon, and Scopophilia: Watching and Being Watched" Pp. 35-54 in *The New Politics of Surveillance and Visibility*, edited by Kevin Haggerty, and Richard Ericson. Toronto: University of Toronto Press.

Lyon, David. 2006b. *Theorizing Surveillance: The panopticon and beyond*. Oregon: Willan Publishing.

Lyon, David. 2009. "Identification practices: state formation, crime control, colonialism and war" Pp. 42-58 in *Technologies of InSecurity: the surveillance of everyday life*, edited by Katja Aas, Helene Gundhus and Heidi Lomell. New York: Routledge-Cavendish.

Marx, Gary. 2003. "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance." *Journal of Social Issues*. 59 (2): 369-390.

Mathiesen, Thomas. 1997. "The Viewer Society: Michel Foucault's 'Panopticon' Revisited." *Theoretical Criminology*. 1: 215-234

Mirowsky, John and Ross, Catherine. 2006. "Social Structure and Psychological Functioning: Distress, Perceived Control, and Trust" Pp. 411-447 in *Handbook of Social Psychology*, edited by John DeLamater. New York: Springer.

Misztal, Barbara. 1996. *Trust in Modern Societies*. Cambridge: Polity Press.

Niedzviecki, Hal. 2009. *The Peep Diaries: How we're Learning to Love Watching Ourselves and our Neighbors*. San Francisco: City Lights Books.

Neyland, Daniel. 2009. "Mundane terror and the threat of everyday objects" Pp. 21-41 in *Technologies of InSecurity: the surveillance of everyday life*, edited by Katja Aas, Helene Gundhus and Heidi Lomell. New York: Routledge-Cavendish.

Ogura, Toshimaru. 2006. "Electronic government and surveillance-oriented society" Pp. 270-295 in *Theorizing Surveillance: The panopticon and beyond*, edited by D. Lyon. Oregon: Willan Publishing.

O'Neill, Onora. 2002. *A Question of Trust*. Cambridge: Cambridge University Press.

Orwell, George. 1962. *Nineteen Eighty - Four*. London: Secker and Warburg.

Putnam, Robert. 2001. *Bowling Alone: The Collapse and Revival of the American Community*. New York: Simon and Schuster.

Robinson, Laura. 2006. "'Black Friday' and Feedback Bombing: An Examination of Trust and Online Community in eBay's Early History" Pp. 123-136 in *Everyday eBay: Culture, Collecting, and Desire*, edited by Ken Hillis and Michael Petit. New York: Taylor and Francis Group.

Rotter, Julian. 1971. "Generalized Expectancies for Interpersonal Trust." *American Psychologist*. 26: 443 - 452.

Rotter, Julian. 1980. "Interpersonal Trust, Trustworthiness and Gullibility." *American Psychologist*. 35(1): 1-7.

Rotter, Julian, Chance, June and Phares, Jerry. 1972. *Applications of a Social Learning Theory of Personality*. New York: Holt, Rinehart and Winston, Inc.

Scott, John and Marshall, Gordon (ed). 2005. *Oxford Dictionary of Sociology*. 3rd ed. New York: Oxford University Press.

Shaw, Sara and Greenhalgh, Trisha. 2008. "Best research – For what? Best Health – For whom? A critical exploration of primary care research using discourse analysis." *Social Science and Medicine*. 66: 2506 - 2519

Smith, Gavin J. 2009."Empowered watchers of disempowered workers? The ambiguities of power within technologies of security" Pp. 125-146 in *Technologies of InSecurity: the surveillance of everyday life*, edited by Katja Aas, Helene Gundhus and Heidi Lomell. New York: Routledge-Cavendish.

Tilly, Charles. 2005. *Trust and Rule*. New York: Cambridge University Press.

Van Swol, Lyn. 2006. "Return of the Town Square: Reputational Gossip and Trust on eBay" Pp. 137-150 in *Everyday eBay: Culture, Collecting, and Desire*, edited by Ken Hillis and Michael Petit. New York: Taylor and Francis Group.

Westen, Drew. 2002. *Psychology: Brain, Behaviour and Culture* (3rd ed). New York: John Wiley and Sons, Inc.

Whittaker, Reg. 1999. *The End of Privacy: How total surveillance is becoming a reality*. New York: The New Press.

Whitty, Monica and Joinson, Adam. 2009. *Truth, Lies and Trust on the Internet*. New York: Psychology Press.

Wilkinson, Iain. 2006. "Psychology and risk" Pp. 25-42 in *Beyond the Risk Society: Critical Reflections on Risk and Human Society*, edited by Gabe Mythen and Sandra Walklate. England: Open University Press.

Wong, Loon. 2008. "Trust in E-Commerce: Risk and Trust Building" Pp. 176-193 in *Computer Mediated Relationships and Trust: Managerial and Organizational Effects*, edited by Linda Brennan and Victoria Johnson. New York: Information Science Reference.

Yar, Majid. 2006. "Cybercrimes and Cyberliberties: Surveillance, Privacy and Crime Control." Pp. 139 – 153 in *Cybercrime and Society*, authored by M. Yar. Thousand Oaks, CA: Sage Publications.

Yamagishi, Toshio. 2001. "Trust as a Form of Social Intelligence" Pp. 121-147 in *Trust and Trustworthiness*, edited by Karen S. Cook. New York: Russell Sage Foundation.

Zedner, Lucia. 2009. "Epilogue: the inescapable insecurity of security technologies?" Pp. 257-270 in *Technologies of InSecurity: the surveillance of everyday life*, edited by Katja Aas, Helene Gundhus and Heidi Lomell. New York: Routledge-Cavendish.