Surveillance, Privacy and the Military

by

Emily Merz

A Paper Submitted to
The Canadian Forces Leadership Institute

Table of Contents

Surveillance, Privacy and the Military

Introduction

In everyday life, public and private organizations, and even our neighbours, increasingly monitor and watch us. Surveillance is being used to coordinate and control human activity. Gary T. Marx coined the term "Surveillance Society" (Lyon: 2001, 32) in 1985 referring to the all-encompassing use of computer surveillance technology in modern society for total social control, while William G. Staples feels that we are becoming a "Culture of Surveillance" (Staples: 1997, 2). Staples defines surveillance simply as "the act of keeping close watch on people" (Staples: 1997, ix). Surveillance functions to monitor and observe groups for the purposes of order, power and social control. We need to question the role of surveillance and its intended and unintended consequences. The increase in surveillance of the population by various organizations raises many moral and ethical concerns, including concerns about personal privacy. Privacy is a difficult term to define, but can be understood as "the right to be let alone" (Young: 1978, 2). If this right to be let alone is imperiled in civil society, it is arguably even more at risk within the military, and our society's increased emphasis on individual rights and personal privacy raises key concerns about the role of military leadership. Traditional obligations to "know one's subordinate" and the assumption of a leader's entitlement to personal knowledge are being challenged. Important questions need to be explored concerning the relationship of surveillance, privacy and personal information in regards to military leadership; questions about the privacy rights of military officers as well as whether or not the existing military system takes active measures to protect these rights. The democratic laws, rights and values of civilian society

need to take precedence over military law and obedience in order to preserve the human rights of military personnel.

The Sociology and Functions of Surveillance

The main function of surveillance is as a form of power and control. In *Surveillance Society: Monitoring Everyday Life*, David Lyon further extends the definition of surveillance to include, "any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered" (Lyon: 2001, 2). This definition includes the motivation behind the collection of data to "influence" or "manage" the data in a particular way. William G. Staples, in *The Culture of Surveillance: Discipline and Social Control in the United States*, writes that surveillance functions as a micro technique of discipline that targets the body as a site to be "watched, assessed, manipulated and enhanced by the use of technologies" that are locally present in the workplace, school, home and community (Staples: 1997, ix). Both these definitions point to the purpose behind surveillance to regulate human activity through technology.

Technologies are central to surveillance in that they allow for it to occur by enabling data to be "stored, matched, retrieved, processed, marketed and circulated" (Lyon: 2001, 2). Lyon sees that surveillance tools were created as means of ordering and government in modern societies that depend on advanced electronic information infrastructures (Lyon: 2001, xi). The complex network of communication and information technologies such as computers and telecommunication support all kinds of monitoring; including computer databases, telecommunications, Internet, video cameras, smartcards, satellite and biometric surveillance

from within the body such as drug testing (Lyon, 2001, 28, 51). This network of communication and information technologies is hidden; nevertheless these modern infrastructures set limits on human activity while also enabling aspects of social life (Lyon: 2001, 29). Modern government administration depends on the collection and recording of personal data while employers depend on surveillance methods to monitor and supervise employees to enhance efficiency and profit. Lyon points to the ways that modern society relies on information and knowledge gathered by surveillance systems in social, economic and political arrangements to maintain power and order in society (Lyon: 2001, 31). Surveillance is used as a form of social management and orchestration to classify, coordinate and control populations (Lyon: 2001, 10).

Although technology allows surveillance to occur at a greatly increased level, it does not create surveillance. Society and technology work together to create a "Surveillance Society", it is not technologically determined. Surveillance occurs in information society amidst technological infrastructures, but is shaped by culture, the level of technological development, political priorities and constitutional arrangements (Lyon: 2001, 29). Technological systems are socially shaped and have social consequences beyond their intentions and can even have effects on social relationships (Lyon: 2001, 24). Technology is not always used for its originally intended purposes. For example, video surveillance in a department store may have been designed to prevent and catch theft, but it may also be used to watch the productivity of the workers. In other words, surveillance technologies that were intended for risk management may also become used as a form of control. Technology is bound to human actors as well as social organizations and structures (Lyon: 2001, 26).

Today, many interactions are performed at a distance through technology, and surveillance relies on abstract data for these interactions. Knowledge based economies relies on personal data for economic, political and cultural functioning. David Lyon believes that we have "disappearing bodies" because we base most of our interactions on bits of fragmented information. Traditionally, human beings interacted face-to-face; now interactions are mediated by technologies such as telephones, computers, faxes, credit cards and the Internet. Relationships now occur without the physical presence of human beings but rather increasingly through electronic means (Lyon: 2001, 15). This creates a society of strangers where one must give tokens of trust and proof of identity in order to demonstrate eligibility and rights to participate in the system (Lyon: 2001, 49). Sharing a similar perspective to Lyon's, Ericson and Haggerty further argue that surveillance serves to abstract bodies from places, causing people to have virtual data-doubles that allow them to participate in the system (Haggerty and Ericson: 2000, quoted in Lyon: 2001b, 1.16).

William G. Staples suggests that surveillance is indicative of a new set of post-modern attitudes, meanings and practices about the nature of human beings, social control and deviance (Staples: 1997, ix). He believes the main reasons for surveillance lie in discipline and social control. That is to say he suggests that the government and private organizations "monitor our performance, gather evidence, assess deviations and extract penalties" in the micro-interactions of everyday life in order to regulate our activities and movements and to shape or change our behaviour (Staples: 1997, 2). Staples feels that the motivation of surveillance is for "law and order, public safety, protection of private property, sound business practice and for individuals' 'own good'" (Staples: 1997, 2). He goes on to call these micro acts of surveillance "meticulous rituals of power", which function for

discipline and social control enhanced by information, communication and medical technologies. Staples feels that surveillance is about power and disciplining people into "normal' action to maintain unbalanced and unequal authority relationships between managers and workers, teachers and students, officers and trainees, etc. (Staples: 1997, 3). In this sense, Staples also argues that surveillance is used for efficient social order and control.

Needless to say, today's disciplinary powers and practices do not occur in a vacuum, but rather spring from our history and culture (Staples: 1997, 9). Surveillance ideas originate back to the Prison Panopticon of 1791 designed by Jeremy Bentham to solve criminal behaviour. The Panopticon consisted of a central guard tower inside a prison or reformatory where the prisoners could not be sure if the guard was watching. Prisoners assumed they were being watched all of the time; the constant observation of the inspector was designed to prevent trouble and produce docility. This "invisible eye" of the authorities allowed for the illusion of constant surveillance. This technique for social control can be applied to any establishment and remains an important symbol of modern disciplinary power and contemporary surveillance techniques (Staples: 1997, 27). The 'unseen observer' of the Panopticon can be recognized in modern forms of 'invisible' electronic surveillance, such as hidden video cameras in public places (Lyon: 2001b, 1.13).

Michel Foucault described such techniques to mould and shape human behaviour and the mind as 'disciplinary power'. Disciplinary power, like the panopticon, is continuous, automatic and anonymous. It is an effective and efficient method of discipline using no physical force or expense, but rather knowledge of actions to exercise power and control (Staples: 1997, 25). This power has benefits for institutions offering efficient supervision for management and control to produce obedience and conformity. Watching others all the time

serves to produce "normalizing judgements" which sort individuals into good and bad and judge people based on their actions. The goal is to produce docile and obedient people for social control. Foucault's ideas suggest that surveillance functions to make people manageable, submissive, teachable and pliable for order, obedience and uniformity (Staples: 1997, 27). William G. Staples argues that we are approaching a new era of discipline and control in the postmodern age; disciplining the whole society to be faster and more effective (Staples: 1997, 31). He sees "surveillance ceremonies" in daily life that monitor, regulate, probe and measure body functions, processes, characteristics and movements as attempting to regulate and control more and more of social life (Staples: 1997, 35).

However, this form of disciplinary power is 'bi-directional' and occurs fragmented throughout the social body. Macro structures of economics, political authority and the state function along with microstructures of everyday life in a matrix of power relations (Staples: 1997, 25). In the 1950's George Orwell predicted a highly co-coordinated, state-driven form of surveillance to occur in his book *Nineteen Eighty-four*. Instead, in today's "Surveillance Society" there is no overarching "Big Brother" watching over us all or totalitarian state control; but rather, many fragmented micro systems at work (Staples: 1997, ix). Surveillance is dispersed through social sectors by public and private organizations. The motives of surveillance are still for order and control, but a much more open-ended surveillance has emerged (Lyon: 2001, 35). For example, there is surveillance for the government for bureaucratic organization, for security and intelligence gathering, for systems of administration and policing, for supervision and monitoring of workers to maximize production as well as to gather consumer data for capitalist consumer management and marketing (Lyon: 2001, 39). Gilles Deleuze and Felix Guattari suggest that the growth of

surveillance technologies are dispersed and decentralized using the metaphor that surveillance spreads like a creeping plant rather than like a tree with a central trunk and spreading branches (Delueze: 1987, quoted in Lyon: 2001b, 1.15). Haggerty and Ericson refer to this looser and freer flowing set of processes as a 'surveillant assemblage' instead of a centrally controlled and coordinated system (Haggerty and Ericson: 2000, quoted in Lyon: 2001, 1.15). Nonetheless, in this dispersed surveillance system, personal data is shared between organizations. Lyon refers to this phenomenon as "leaky containers" (Lyon: 2001, 37). Data routinely flows freely between sectors, blurring the boundaries between sectors that handle personal information (Lyon: 2001, 45).

David Lyon asserts that the sorting which occurs from surveillance is crucial to life chances and that it creates many ethical and political concerns (Lyon: 2001, 10). He sees that surveillance reinforces social differences and divisions and affects life chances through categorization and risk management (Lyon: 2001, 25). People are constantly risk-profiled and sorted into consumer categories by commercial surveillance and into social dangerousness categories by policing and intelligence systems (Lyon: 2001). This type of surveillance sorting can lead to discrimination and exclusion from the system. Lyon believes that the abstract data of surveillance reinforces familiar divisions based on factors of social class, race, ethnicity, gender and sexuality; categories are created to assess behaviour and include or exclude (Lyon: 2001, 49). For example, certain categories of people are red flagged by surveillance cameras monitoring for theft in department stores, such as teenagers and visible minorities. This means that solely based on physical appearance certain groups of people are suspect and classified into deviant categories.

Lyon also suggests that surveillance technologies have two faces. The first is their goal to protect and control societies through risk management as well as for efficiency and convenience. Surveillance systems are designed to anticipate and prevent danger and make citizens feel safe (Lyon: 2001, 45). The other face is the cause of risk and fear and loss of the protection of privacy (Lyon: 2001, 2). The unwarranted intrusion into private life for the purposes of government organization, commercial control of personal consumption or social control is the negative impact of surveillance technologies (Lyon: 2001, 45). This face causes risk to personal privacy and also the factors of discrimination and exclusion mentioned above. These two faces can also be referred to as the 'double-edged sword" of surveillance. The many negative effects of surveillance, such as loss of privacy and reinforcement of social divisions, are sacrificed for the benefits of risk management, protection, convenience and social order (Lyon: 2001, 2).

Privacy Concerns

One of the greatest ethical concerns of the increased use of surveillance throughout society is its effect on personal privacy. Gary T. Marx, a sociologist at the University of Colorado, is concerned that new technologies that collect personal information probe more deeply and widely into personal lives and transcend previous barriers. He argues that personal boundaries are increasingly permeable by the government and private organizations with lack of awareness and consent by individuals giving cause for great concerns for personal privacy (Marx: 1998, 171). David Flaherty, a historian and the former Privacy Commissioner of Canada, argues that the constant surveillance through public and private sector databases has

many negative implications for the quality of human rights. He believes the search for personal security, efficiency and profit in our "Surveillance Society" is threatening privacy (Phillips: 1996). Surveillance technologies have served to blur the boundaries between the public and private aspects of individual human life.

Privacy is a difficult term to define. John B. Young, from the Department of Economics at the University of Southampton, says it best when he refers to privacy as a more recognized term than a described one (Young: 1978, 3). The Younger committee set out to study the history of privacy in 1972 and found that "the concept of privacy cannot be satisfactorily defined" with one single definition but that it is "of great importance" (Velecky: 1978, 18, 20). However, many people have attempted to define the term privacy. The most universal definition of privacy is that of Brandeis from 1890, which is "the right to be let alone", he goes on to refer to privacy as "the most comprehensive of rights, and the right most valued by civilized man" (Young: 1978, 2). Warner describes privacy as "the right to be free of interference in fairly trivial affairs" (Velecky: 1978, 20). Sisella Bok calls privacy the "condition of being protected from unwanted access by others- either physical access, personal information or attention" (Ekos: 1992, 1). While these definitions point to protections from unwanted intrusions, a more positive definition of privacy would include "to be the captain of [our] soul[s]", meaning to have the power to actively control contact with others (Young: 1978, 8). Other words used to describe privacy include: anonymity, solitude, intimacy, reserve, freedom, free choice, democracy, autonomy, confidentiality, self-direction and control of one's own affairs. In sum, individuals in western liberal democracies have a natural desire for some mental privacy that must be preserved from intrusion by others (Young: 1978, 3).

Despite the ambiguity in the term's meaning, privacy is a recognized fundamental human right with importance connected to human values. Privacy is a social human right and relates to the role of the individual in the community. Some loss of privacy is inevitably required to participate in the public system and is necessary for the common good (Young: 1978, 2). For example, people must give up privacy when providing their Social Insurance Number in order to achieve the benefits of work, or must give up personal credit information to obtain a credit card to have buying privileges. In other words, to participate in the efficient functioning of public bureaucracy, with private corporations for a better consumer economy and for more productive workplaces, individuals must give up some private information (Young: 1978, 12).

The freedom and privacy of individuals must also be balanced with security measures of the state in order to deal with the discipline of deviance. Accordingly, John B. Young suggests that privacy is an inherent right, yet individuals must strike a balance between their own personal privacy and state discipline and justice. For instance, a reasonable amount of privacy must be sacrificed for protection and prevention of crime, such as giving fingerprints for police records so that they can detect criminals in theft cases (Young: 1978, 10). On the extreme end of crime prevention, complete loss of privacy from imprisonment is the primary aspect of punishment in Western society (Young: 1978, 10). Many legal and social safeguards are in place to prevent the misuse of government power. For example, the criminal justice system, which uses prosecution and defense lawyers to represent clients before a judge and jury in court, is used as a system of checks and balances in efforts to prevent the wrong people ending up in jail. Although these safeguards often fail, they are evidence of our culture's respect for privacy as an ideal.

However, while some loss of privacy has always been necessary for the efficient maintenance of liberal democracies, government and commercial surveillance of personal information has recently increased to the point where surveillance is everywhere and we are giving up far too much privacy to be part of the social system. Simon Davies argues that government and private organizations now have a general search warrant on the entire population (Phillips: 1996). All people are being watched all of the time using surveillance systems that are greatly threatening individual privacy. Surveillance systems were designed as a solution to protect individuals but instead are inhibiting normal activities and limiting individual freedoms. For example, placing video surveillance cameras in public places watches all citizens without necessarily reducing the amount of crime (Phillips: 1996). Corporations and government use surveillance technologies as a form of risk management that categorizes and may exclude many individuals from participating in society and the economy. Michel Foucault would have seen the extension of surveillance throughout society as a form of social control of the public by the government and private sector to control everyday life (Whitaker: 1999, 1).

These threats to personal privacy have only increased since the terrorist attacks on September 11th, 2001 in New York and Washington. David Lyon fears that the increases in surveillance after the attacks may further impede the civil rights of citizens who will be more profiled and screened by many increases in high tech security systems (Lyon: 2001b). Extensive anti-terrorist legislation designed to protect citizens has led to increased policing and security services, in both commercial and government sectors. Increased airport security devices as well as video camera monitoring in public spaces are leading to greater monitoring of citizens. Lyon argues that these technical fixes are not the answer to preventing such

attacks from happening again; instead they serve socially negative effects by emphasizing public control over protection of individual privacy rights (Lyon: 2001b). In the aftermath of the attacks, there is a tendency to rely on technological enhancements to surveillance systems before it is clear whether or not they even work to solve the problem for which they are implemented (Lyon: 2001b). For example, facial recognition devices have been implemented in some airports to target fliers with a criminal record, but it is not yet clear whether or not these devices are effective at identifying suspects by their image. Police and intelligence services have been granted greater powers to extend their surveillance capabilities, giving governments more control over citizens' rights. Lyon questions 'how new' and 'how necessary' these measures are and points to the lack of knowledge on whether or not these new technologies work as they are supposed to, not to mention the unintended and possibly irreversible consequences that are yet unknown (Lyon: 2001b). Intrusion and exclusion may be the result of extended surveillance threatening personal privacy and reproducing and reinforcing social, economic, and cultural divisions in society. Lyon suggests there is lack of informed sociological comment on these far-reaching developments (Lyon: 2001b). Focusing on technological solutions may not be the answer to preventing further terrorism. Ethics and democracy should guide surveillance practices, not fear.

If the attacks on September 11th changed North American attitudes towards surveillance and privacy, what characterized those attitudes before the attacks? The *Canadian Privacy Survey* provides some answers to this question. The *Privacy Survey* in 1992 uncovered Canadian public opinion about privacy. The *Survey* included 3,000 households and found pervasive public concern over privacy with 92 percent of respondents at least moderately concerned over privacy and 52 percent with extreme concerns (Ekos: 1993, i).

Eighteen percent claim to have experience a 'serious privacy invasion', which includes robbery, assault, intrusions, requests for information in the home and psychological and verbal harassment; suggesting the high rate of privacy concerns are not necessarily based on personal experiences, however, they are still valid (Ekos: 1993, i). Canadians demonstrated higher concerns over privacy than U.S. comparisons (Ekos: 1993, i). Interestingly, the technologically literate experienced higher comfort levels. The *Survey* concluded that technological, commercial and social threats have caused people to believe there is significantly less privacy than before (Ekos: 1993, 40). The *Survey* concludes that the impersonality of modern society, rapid technological change and socioeconomic changes accompanied by increasing requests for personal data have led to the feeling of a loss of privacy (Ekos: 1993, 40). The *Survey* also states that a more active role needs to be taken by individuals to shape their personal privacy, but 60 percent of those surveyed do not know where to turn with a privacy problem. Public opinion in this survey suggested the need for more government regulation and control of privacy rather than self-regulation (Ekos: 1993, 46).

Despite the described public concern over threats to personal privacy through surveillance, little protest against the invasion of privacy by the public has occurred. Reg Whitaker suggests that this is due to the fact that the public is often only told the rewards of many surveillance technologies and not the negative aspects that may result from them (Whitaker: 1999, 3). For example, citizens are bombarded with the many benefits of owning a credit card for purchasing power and convenience, but are only told in fine print that the information that they provide to receive a card can be sold to other companies, making them targets for further soliciting. Another convincing argument for the use of surveillance

technologies is that individuals have nothing to worry about if they have nothing to hide (Phillips: 1996). However, Bruce Phillips, the Privacy Commissioner of Canada in 1996, argues that even if one has nothing to hide, one does have a great deal to lose, such as autonomy, anonymity, and rights to go about daily duties without interference, not to mention dignity and control over one's life. He also suggests that surveillance alters behaviour in subtle ways (Phillips: 1996). We need to be reminded that privacy is a core value of democratic rights that needs to be protected for democracy and ethics (Phillips: 1996).

While surveillance technologies heighten concerns about privacy, the real threats lie less in those technologies than in the people who operate them. People decide how to implement surveillance technologies and decide for what purposes they will be used. Little public discussion occurs before implementation of new surveillance practices. Bruce Phillips sees a shift in public mood toward implementing "personal security at all costs, security at any cost" (Phillips: 1996). What this means is a general public feeling that increased implementation of technological devices will prevent crime, which results in law enforcement and public security coming before privacy rights. Additionally, Phillips recognizes the government's use of surveillance technologies and data matching and sharing practices to increase efficiency and reduce costs of operation taking precedence over privacy. Finally, Phillips points to the money driven incentives of the high technology industry to sell their products as security enhancing devices. These companies use persuasive arguments about many social problems that may not even exist or be as terrible as they claim, such as drug use, and without mentioning the damages of implementing these technologies on personal privacy. All of these new technologies are implemented at the cost of losing a certain amount of personal privacy (Phillips: 1996). Technologies are implemented slowly, many isolated

incidents become a slippery slope to loss of privacy making it difficult to pinpoint where the problem began. This suggests the need for active direction and regulation on how surveillance is used in order to create adequate safeguards for privacy.

With the high levels of surveillance used by governments and commercial organizations, individuals want to be able to control how information about them is used. In our information society, data profiles about individuals are largely out of our personal control and may actually overshadow and oppress our real circumstances (Whitaker: 1999, 2). Government and private corporations possess detailed databases of private information on individuals, which Reg Whitaker refers to as "dataveillance" (Whitaker: 1999, 2). Data protection deals with the control of the "collection, use and dissemination of personal information" (Flaherty: 1996, xiv), while privacy protection includes a broad range of various forms of intrusive behaviour. Data protection is a critical component of privacy protection because it involves the protection and limiting of data collection by automated surveillance databases, helping to preserve individual privacy (Flaherty: 1989, xiv). Bruce Phillips comments that the control of personal information is necessary for privacy and that once it is lost it cannot be regained (Phillips: 1996).

Legal Issues of Privacy

As we have seen, privacy may be difficult to define, yet it is recognized internationally and in Canada as a fundamental human right and is regulated under international conventions, constitutional law, federal and provincial legislation and professional codes of conduct (Phillips: 1996). The Universal Declaration of Human Rights states that everyone has "the right to life, liberty and security of the person" (Phillips: 1996).

The Universal Declaration also states that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation" (Phillips: 1996). Section 7 of the Canadian Charter of Rights and Freedoms also guarantees 'the right to life, liberty and the security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice" (Phillips; 1996). Additionally, the Canadian Charter guarantees "the right to be secure against unreasonable search or seizure" in section 8 (Phillips: 1996). The Charter is used in Canada to protect privacy in criminal law as well as outside the criminal context. In a Supreme Court of Canada criminal appeal of *R. v. Edwards*, Mr. Justice La Forest suggested that section 8 of the Charter "draws a line between the rights of the state and the rights of the citizen, and not just those of an accused. It is a public right, enjoyed by all of us" (Phillips: 1996). Furthermore, Canada is one of 22 other industrialized nations that are part of *The Organization for Economic Co-operation and Development's (OECD*) *Guidelines for the Protection of Privacy and Transborder Flows of Personal Data.* These guidelines were created in 1984 to protect the privacy of personal data only in the public and private sectors; they established minimum standards for handling personal information to harmonize data protection laws and practices among OECD member countries. These guidelines are, however, voluntary and are not legally binding (Phillips: 1996).

Before the 1970's the right to personal privacy was not specifically addressed in Canadian law. In the early 1970's a task force was created for privacy and computers with a committee on privacy, when the public knew little about threats to personal privacy by new technologies (Flaherty: 1989, 246). Privacy was first regulated under the Human Rights Act of 1977, which created the post of privacy commissioner and introduced fair information

practices in the federal public sector. This Act was expanded upon in 1983 with the creation and implementation of the Federal Privacy Act (Flaherty: 1989, 243). The purpose of the Privacy Act "is to extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution" (Privacy Act: 2002). This federal data protection legislation is designed to restrict government surveillance of citizens by regulating the government's collection, use and disclosure of personal information about Canadians (Flaherty: 1989, 253). The Act has provincial counterparts in all provinces, except New Brunswick, to regulate personal data collection by the provincial and municipal governments (Phillips: 1996). The "Chronology of Canadian Federal Data Protection Legislation" can be seen in Appendix A (Flaherty: 1989, 244).

The Privacy Act contains a detailed code of fair information practices to guide the collection, retention, disposal and protection of personal information (Flaherty: 1989, 253). For example, individuals must be informed about why data is being collected from them and it must be limited to that use; information must come directly from individuals; and they must be given the choice to provide it (Flaherty: 1989, 254). There are 13 conditions specified under the Act that authorize information disclosures, such as consent. Information must also be kept accurate, complete and up to date and must be disposed of if it is no longer needed. Additionally, the Act specifies that the collection of information should be for efficiency in government operation and not for unnecessary purposes. These guidelines are designed to give citizens the right to control the disclosure of personal information about themselves and to prevent government misuse of that information (Flaherty: 1989, 255).

Gary T. Marx points out that the Principles of Fair Information Practices, as those mentioned above, are no longer adequate because they are three decades old and need to be broadened to take into account new technologies that collect personal information, not just computers. Some examples of these new technologies would include DNA and drug testing, hidden video cameras, electronic location monitoring using implanted chips, Internet monitoring devices, smart cards that contain extensive personal information and satellites (Marx: 1998, 171-172). Marx suggests that a broader set of ethical principles is needed to actively guide all forms of technological data collection and use. He presents 29 questions that when answered effectively would serve as a general framework to ethically guide the use of surveillance technologies, by judging the context and conditions of data collection as well as the uses and goals that they are trying to meet. These 29 questions, entitled "Questions to Help Determine the Ethics of Surveillance" can be seen in Appendix B. Marx argues that in order to protect a reasonable degree of personal privacy certain conditions must be met. A central factor is reasonable respect for the dignity of the person and emphasis is placed on the avoidance of harm, validity, trust, notice, and permission when crossing personal borders (Marx: 1998, 171). These principles represent an active approach to ethically guiding the use of surveillance technologies to protect individual privacy.

The Privacy Act has also served to strengthen the investigation and auditing of privacy concerns. Under the Act, the Privacy Commissioner was given a more active advisory role in difficult cases of government surveillance. The Commissioner has the authority to investigate and monitor government surveillance as an independent entity to balance the public interest and individual privacy with information handling of government departments to make sure that they comply with fair information principles (Flaherty: 1989,

247). David H. Flaherty argues that in order to be effective in limiting government surveillance, data protectors must be independent entities, must have the power to intervene and must also be willing to use these powers; the Privacy Commissioner of Canada possesses these powers (Flaherty: 1989, 259).

While the Privacy Act serves an important function in protecting the personal privacy of Canadians, there is still room for improvement with its implementation. Flaherty points out that the Act only protects privacy against government organizations and does not protect individual privacy in the private sector or commercial corporate world; the private sector is still self-regulated, leaving room for many infringements on privacy (Flaherty: 1989, 297). The Canadian Standards Association has created a voluntary code of privacy protection for the private sector, but there are no laws making it mandatory for compliance (Phillips: 1996). Canadian privacy laws also have not kept up with technology, meaning many technological applications have not been addressed by the Canadian legal system and are therefore unregulated (Phillips: 1996).

As Reg Whitaker suggests, technology and surveillance are causing individuals to be more and more transparent, making the private spaces of individual refuge disappear, which is leading to great public concern (Whitaker: 1999, 3). Increased regulation and checking procedures are needed to safeguard against individual privacy invasions from the rapid spreading of information and surveillance technologies. In order to gain or maintain control over personal information, the public must be given the right to provide personal information based on informed consent, and must be given advanced notice when personal information is collected and told for what purpose it will be used. The current safeguards, while having their

advantages, are not adequate safeguards to protect privacy. More formal rules are needed in both the public and private sector, such as the 29 questions proposed by Gary T. Marx.

Additionally, however, the public also has an active role to play. Individuals can make small-scale protests against unneeded disclosures of personal information, such as refusing to provide Visa numbers over the phone in order to purchase a product. These micro protests may lead government and private organizations to rethink their necessity for these invasions. Bruce Phillips points out that the public needs to have access and knowledge about privacy encryption devices to actively protect themselves against intrusions. The public needs to be informed about how their privacy is being infringed upon and how they can actively protest against it. Access to privacy enhancing technologies should be free and already built into technologies as the default (Phillips: 1996).

Bruce Phillips also points out that more surveillance does not mean a better, more secure society, but instead may mean the opposite. We need to appreciate individual privacy when implementing new surveillance technologies (Phillips: 1996). There may be other solutions to implementing surveillance technologies that do not infringe upon privacy rights that may be equally effective. For example, instead of testing employees for use of illicit drugs, performance testing could be used to test whether or not employees can do the job effectively. Individuals should not always have to sacrifice privacy to implement technology. The public must actively guide surveillance technologies to control how we want them to be used, not just use them because they are available.

Surveillance and Privacy in the Military

Surveillance and loss of privacy are an inherent part of participation in the Canadian Forces. The military is a site of extreme surveillance, both social and technological. Most surveillance technologies originated in the military and spy agencies (Wood: 2001, 18). Computer based information infrastructures began in the military (Lyon: 2001, 29), for example the creation of the Internet in 1960's. These technologies were designed for command and control and used for what Michel Foucault refers to as 'disciplinary power'. The military presents a distinct category of intense surveillance, where intrusions into the private life of military personnel are a daily occurrence.

The military is a unique group that differs from the rest of society. Captain Donald A. Neill suggests that what distinguishes the military profession from other professions is its ethical codes where there is "voluntary subordination of one's own interests to those of the state" (Neill: 2000). Military life consists of hierarchical organization where the group is placed above the individual and where work, home life and leisure time are all connected in a full time commitment to the military way of life. Thomas E. Ricks, a journalist specializing in the military institution, suggests that soldiers and their families give up many freedoms in order to participate in this unique society (Ricks: 1996).

The military creates this unique form of controlled society upon entrance. Dr. Peter G. Bourne, a doctor of Psychiatry and previous captain in the U.S. Army, states that many psychological and sociological effects occur upon individuals during basic training for the military. He suggests this training separates training officers from civilian life in order to shape new spirit, attitudes and philosophies of the military. This military system is designed to develop disciplined and motivated soldiers with weapons training, physical conditioning

and soldiery. Bourne argues that basic training causes a social and psychological shock that transforms trainees' identities, values and allegiance to be consistent with the military (Bourne: 1971, 138). Arthur Schafer, writing for the Commission of Inquiry into the Deployment of Canadian Forces to Somalia, supports these claims by arguing that an individual's identity is shaped by the institutional norms and structures of the military through a powerful and prolonged military socialization process. Schafer continues that this new group identity can override prior socialization and values of civilian culture (Schafer: 1997).

The military creates this unique social system because of its special function to protect society from external threats of violence (Schafer: 1997). Obedience to authority and loyalty to comrades are the highest military values. Arthur Schafer argues that unquestioning obedience is the highest military virtue because "military necessity" requires that soldiers act quickly in order to prevent tragedy; delay or hesitation could result in fatalities (Schafer: 1997).

As with other surveillance practices, this controlled way of life and discipline has many benefits for the functioning of the military. Schafer argues that instant obedience and complete loyalty create an efficient military force that can effectively protect society against external military threats (Schafer: 1997). Additionally, Thomas E. Ricks argues that the U. S. Fort Drum army base is drug free and has better race relations than any other social institution in the U. S. (Ricks: 1996). The military system of obedience clearly has benefits for order, control and efficiency of military personnel. However, since surveillance practices always present a double-edged sword of benefits and negative consequences, the latter will be outlined next.

In addition to conferring benefits on the group, the controlled way of life in the military leads to a loss of privacy for military personnel. Major Leslie Nepper of the Fort Drum army base in the United States comments that "there is not an awful lot of privacy in the military- it's kind of a goldfish bowl" (Ricks: 1996). For example, these soldiers are subject to HIV tests every 2 years, they live in houses on base that are governed by base regulations and have their own policing systems inside the base. The standards of the base affect their personal and home lives as well as their lives as military service people (Ricks: 1996). Robert S. Rivkin suggests, in *GI Rights and Army Justice: The Draftee's Guide to Military Life and Law*, that military personnel often forget their individuality and do not think of having privacy in the military. Rivkin writes that commonly accepted privacies are labeled as 'privileges' to be given or withheld by higher military ranks (Rivkin: 1970). Higher ranked officers are allowed more privacy while the lower ranked officers have the least privacy. For example, senior ranked officers have their own rooms, sometimes off post, while lower ranked officers must share living quarters and bathroom facilities with many other officers and are subject to room inspections and other invasions of personal privacy. Passes for leave depend on seniority and can be withheld (RMC: 2002). Schafer comments that the highly authoritarian structure of the military serves to systematically make military personnel vulnerable to abuse of power (Schafer: 1997). Rivkin recognizes that privacy enhances human dignity and individuality by placing limits on government authority and public knowledge of individuals (Rivkin: 1970).

Military personnel are both citizens and soldiers and must abide by civilian laws as well as military laws. The Canadian system of military justice is regulated under the National Defense Act R.S.C. 1985, amended in 1998, which is a legal statute of Canada passed by

federal governmental powers to provide for National Defense. The National Defense Act contains a subsection under Part 3 called the Code of Military Service Discipline that establishes the jurisdiction of the Canadian Forces in dealing with services offenses and punishment. These laws apply to the military service in times of peace and conflict, in Canada and abroad and while in uniform or on duty. All members of the Canadian Forces, including the navy, airforce, and army are subject to these separate and distinct laws as well as all other laws in Canada (JAG: 2002).

The Judge Advocate General's office explains the need of the Code of Military Service Discipline in the National Defense Act as a separate justice system to enforce discipline in the military. The Supreme Court of Canada states in the case of *R. v. Genereux,* [1992] 1 S.C.R. 259:

> "The purpose of a separate system of military tribunals is to allow the Armed Forces to deal with matters that pertain directly to the discipline, efficiency and morale of the military. The safety and well being of Canadians depends considerably on the willingness and readiness of a force of men and women to defend against threats to the nation's security. To maintain the Armed Forces in a state of readiness, the military must be in a position to enforce internal discipline effectively and efficiently. Breaches of military discipline must be dealt with speedily and, frequently, punished more severely than would be the case if a civilian engaged in such conduct. As a result, the military has its own Code of Discipline to allow it to meet its particular disciplinary needs" (JAG: 2002).

The Supreme Court points to a need for a separate system of laws for the military to enforce discipline efficiently because of their special tasks to maintain readiness to defend against threats to national security (JAG: 2002). The Supreme Court points out that ordinary civilian courts are inadequate to serve these needs of the military because they require a quicker and more severe punishment in order to achieve their tasks. The military justice system is made up of informal summary trials with no lawyers and limited punishments to discipline minor service offences and formal courts martial trials involving military judges, prosecutors and

defense council like civilian courts for more serious offences. Both forms of trial can be held wherever forces are deployed (JAG: 2002).

In Canadian law, the Constitution of Canada including the Charter of Rights and Freedoms takes precedence over all other statutes in Canadian law, including those of the military. This means the National Defense Act and the Code of Military Service Discipline contained within the Act are subject to the provisions of the Charter (JAG: 2002). In democratic society, military laws are subordinate to the higher principles and laws of the country. Obedience to civilian laws and the Constitution are more important than military obedience. Schafer argues that in the hierarchical authoritarian organization of the military, the highest value must be placed on obedience to the law and civilian control, so as not to undermine the civic society and democratic values that the military stand for in the first place (Schafer: 1997). In other words, the rule of law requires civilian control over the military (Schafer: 1997).

However, while the rule of law may take precedence in theory, Dr. Peter G. Bourne argues that "military training and organization embody the concrete realization of attitudes and activities that are diametrically opposed to the practice and spirit of democracy" (Bourne: 1971, 153). In other words he argues that obedience is the key aspect of military order which is the opposite to the democratic values of free expression of opinion and right to question actions that are held by citizens. Schafer supports this claim by commenting that liberal democracy places central importance on the individual, autonomy and openness that contrasts with the inherent nature of military organizations to place emphasis on group loyalty, rigid obedience to superior orders and strict discipline (Schafer: 1997, 29). The military system of silent acceptance of authority and group dynamics is inconsistent with democratic society of

active participation in decision making and policymaking process (Bourne: 1971, 153). Military personnel must accept discipline without challenge and accept the military organizational identity and values for control and discipline which is against the values of freedom and democracy that the military serves to protect, which creates tension (Bourne: 1971, 157).

However, one must question whether the special function of the military to defend society takes priority over the human rights of officers. Certain privacy rights are often sacrificed in the military for order and discipline because of the special socialization processes and functions of the military previously mentioned. Robert Sherrill, a critic of the U.S. military system, points out that "military necessity" is often used to justify the loss of personal human rights, including privacy, in the military to achieve order, discipline and conformity in preparation for war (Sherrill: 1970, 224). The military is in a unique group in society with their own laws and standards because of their special situation and function of military preparedness and defense preparation. Military personnel live separately from civilians, creating alienation from the civilian system. Extra powers of punishment are given in the military for discipline and control. While military personnel are guaranteed the same human rights as civilians, they must give up many of these rights when they enter the military, including a degree of privacy. Unlike civilians, military personnel are not likely to complain because of the intense loyalty that they have developed toward military doctrines. Schafer argues that because the military system is based on trust and loyalty of soldiers, officers and superiors, they must have confidence in the system and will therefore not likely challenge it for privacy rights because criticism of the system would be disloyal (Schafer: 1997).

James Finn, author of *Conscience and Command*, argues that citizens leave one society for another when they join the armed forces; in essence, that citizens leave behind constitutional rights of civil society for military justice when they enter the military (Finn: 1971, 3). There are additional rules and regulations that are enforced in the military that are not civilian. The military courts often grant much control to military commanders in the extent that they can control the welfare, safety, morale and effectiveness of their troops (Rivkin: 1970). The special structures, doctrines operating procedures, methods of training and discipline as well as a distinct system of military justice allow the military to maintain discipline and prompt compliance with superior officer's orders (Finn: 1971, 5). Finn states that military justice acts as a deterrent to undesirable behaviour and allows for organizational effectiveness and control (Finn: 1971, 5).

By contrast, Robert Sherrill argues that military personnel are citizens first and soldiers second (Sherrill: 1970). He believes that military personnel should be guaranteed the same human rights as civilians and that we should not govern the military in a separate category. Accordingly, Chief Judge Robert E. Quinn of the United States Military said in U.S. v. Milldebrandt that, 'persons in the military service are human beings endowed with legal and personal rights which are not subject of military order' (Rivkin: 1970, 146). Finn argues that the choice between effective fighting and human rights in the military may not be necessary (Finn: 1971). There may be more effective ways to carry out order, discipline and authority that do not involve infringing on the human rights and privacy of officers. There is a delicate balance between the rights of officers as civilians under the Charter versus the rights of officers in the military under military doctrines and laws. The human rights and freedoms of service people need to be preserved, and should be preserved as the Constitution

overrides the National Defense Act. Military personnel should not be in a separate category. We may not need to make the separate distinction of military and civilian laws. There may be other methods of order and discipline that are less harsh that would better protect human rights and still be effective, presenting a topic for further exploration. Military personnel should be treated as civilians with the same rights (Sherrill: 1970).

The inconsistencies between traditional military values and contemporary social and legal civil society also cause one to question whether or not these differences are necessary. Should the military be able to impose its own unique system of rules and discipline? Thomas E. Ricks suggests that methods of training new soldiers are becoming more humane and are preserving the dignity of trainees, including privacy, by using less discipline. He feels this is necessary in order to have more volunteers participate in the military system (Ricks: 1996). Schafer argues that the traditional culture of the military needs modification in these 'peacetimes'. He continues that the military traditions are dislocated from the caring, compassionate and politically correct Canada that it serves (Schafer: 1997, 29).

Conclusion

It has been demonstrated that the vast increases in technological surveillance in society as a whole are leading to great concern over personal privacy. In an era of extreme surveillance by public government organizations, private business corporations and individuals, it is becoming increasingly difficult to preserve personal privacy over information about the self as well as protection from unwanted invasions. Many laws and regulations have been created in order to protect and preserve individual privacy rights;

however, a more active approach is needed to guide technological surveillance and prevent privacy intrusions from occurring in the first place. In order to protect privacy, legal methods of monitoring, criticizing, contesting and checking government and private sector powers of surveillance need to be in place. A system of checks and balances will serve to limit the consequences and implications of surveillance. The current system of privacy protection in Canada is not completely effective in that it has not kept up with technological advances and does not legally regulate the private sector, leaving room for many privacy invasions.

The concerns over surveillance and privacy in society as a whole raise additional questions about the privacy rights of military personnel. The military represents a unique section of society with its own rules, laws and order. It is the site of the most extreme surveillance practices, as surveillance originated in the military. Military officers are guaranteed the same rights as civilians under the Charter of Rights and Freedoms, which is the supreme law of the land, but are also judged separately in their own justice system. Military personnel are supposed to have the same privacy rights as civilians, but they remain in a distinct category that uses surveillance practices as disciplinary power for an effective and obedient Canadian Forces. The extreme forms of discipline and regiment in the military are accepted because of their unique function in Canada to defend the county in times of war. Military personnel often sacrifice personal privacy in order to participate in this unique organization.

Nevertheless, military officers should have the same privacy rights as civilians in a democratic system. The military system of discipline and rules require reevaluation to protect the human rights of military officers and to preserve the democratic values that the

military serves to protect. As a public organization, the military has the responsibility to protect the individual privacy and dignity of their personnel by actively guiding the use of surveillance with knowledge and ethics. The laws and organizational policies of the military must take into consideration the ethics of fair information practices, including how information about military personnel is collected and used. Further, they must protect against unwanted intrusions. As Gary T. Marx suggested, respect for the dignity of the person, and emphasis on the avoidance of harm, validity, trust, notice and permission when crossing personal borders should be of the utmost importance (Marx: 1998). Responsible surveillance of military personnel should include the minimization of its use and must clearly define what is needed for 'military necessity', taking into account if there are other appropriate means available to accomplish the task. The military must prevent the misuse of power and technological surveillance before it is implemented. The use of surveillance for disciplinary power should be actively guided by people to protect human rights of privacy in the military, as in society as a whole, rather than reacting to problems and infringements after the damage has already been done.

Appendix A

Source: Flaherty, David H. (1989*). Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the U.S.* Chapel Hill: University of North Carolina Press, p. 244.

Appendix B

Source: Marx, Gary T. (1998). “Ethics for the New Surveillance”, *The Information Society*, Vol. 14, pp. 174.

Bibliography

Bourne, Peter G. (1971). "The Military and the Individual", in James Finn, Conscience and Command: Justice and Discipline in the Military, New York: Random House.

D-Net (Canada) (2002). *National Defense of Canada*, Minister of Public Works and Government Services, http://www.dnd.ca

Ekos Research Associates (1993). Privacy Revealed: The Canadian Privacy Survey. The Government of Canada.

Finn, James (1971). Conscience and Command: Justice and Discipline in the Military, New York: Random House.

Flaherty, David H. (1989*)*. Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the U.S. Chapel Hill: University of North Carolina Press.

Halperin, Morton H. and Daniel Hoffman (1977). Freedom vs. National Security: Secrecy and Surveillance, New York: Chelsea House Publishers.

JAG (2002). *Office of the Judge Advocate General*, http://www.forces.ca/jag/dyk_1_e.html

Lyon, David (2001). Surveillance Society: Monitoring Everyday Life, Philadelphia: Open University Press.

Lyon, David (2001b). "Surveillance after September 11", *Sociological Research Online*, Vol. 6, No. 3, http://www.socresonline.org.uk/6/3/lyon.html

Lyon, David and Elia Zureik (eds., 1996). Computers, Surveillance, and Privacy. Minneapolis: University of Minnesota Press.

Marx, Gary T. (1998). "Ethics for the New Surveillance", *The Information Society*, Vol. 14, pp. 171-185.

Neill, Captain Donald A. (2000). "Ethics and the Military Corporation", *Canadian Military Journal*, Vol. 1, No. 1, Spring, http://www.journal.dnd.ca/vol1/no1_e/milethics_e/eth1_e.html

Phillips, Bruce (1996) "Dr. Bernie Vigod Memorial Lecture", Nov. 7, *Privacy Commissioner of Canada*, http://www.privcom.gc.ca/speech/archive/02_05_a_961107_e.asp

Privacy Act (2002). *Privacy Commissioner of Canada*, March 12, http://www.privcom.gc.ca/legislation/02_07_01_e.asp#002

Reagan, Pricilla (1995). Legislating Privacy: Technology, Social Values and Public Policy, Chapel Hill: University of North Carolina Press.

Ricks, Thomas E. (1996). "The Great Society in Camouflage", *The Atlantic Monthly*, Vol. 278, No. 6, Dec, pp. 24-38, http://www.theatlantic.com/issues/96dec/military/military.htm

Rivkin, Robert S. (1970*).* GI Rights and Army Justice: The Draftee's Guide to Military Life and Law, New York: Grove Press.

RMC (2002). *Royal Military College of Canada*, http://www.rmc.ca

Schafer, Arthur (1997). The Buck Stops Here: Reflections on Moral Responsibility, Democratic Accountability and Military Values: A Study, Ottawa: Commission of Inquiry into the Deployment of Canadian Forces to Somalia.

Sherrill, Robert (1970). Military Justice is to Justice as Military Music is to Music, New York: Harper & Row Publishers.

Staples, William G. (1997). The Culture of Surveillance: Discipline and Social Control in the United States, New York: St. Martin's Press.

Valecky, Lubor C. (1978) "The Concept of Privacy" in Young, John B. Privacy, Toronto: John Wiley & Sons.

Watson, Bruce Allen (1997). When Soldiers Quit: Studies in Military Disintegration, Westport, Conn.: Praeger.

Whitaker, Reginald (1999). The End of Privacy: How Total Surveillance is Becoming a Reality, New York: New York Press.

Wood, Chris (2001). "Do You Know Who's Watching You?" *Maclean's*, Vol. 114, No. 8, pg. 18-23.

Young, John B. (1978). Privacy, Toronto: John Wiley & Sons.